SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez, State Bar No. 279017
Mahnam Ghorbani, State Bar No. 345360
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law
ramirez@kiesel.law
ghorbani@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted *pro hac vice*)
The Helmsley Building
230 Park Ave, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
Jallé H. Dafa, State Bar No. 290637
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE I, *et al.*, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC.

Defendant.

This document applies to: All Actions

Case No.: 3:23-cv-02431-VC
Consolidated with: 3:23-cv-02343-VC

REBUTTAL DECLARATION OF DR. ZUBAIR SHAFIQ IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Judge: Hon. Vince Chhabria
Date: September 21, 2023
Time: 10:00 AM
Ctrm: 4, 17th Floor

REBUTTAL DECLARATION OF DR. ZUBAIR SHAFIQ

1. I have been retained by counsel for Plaintiffs as an expert in this matter.
2. I previously submitted a declaration[1] in support of Plaintiffs' Motion for Preliminary Injunction, dated June 12, 2023, which sets out my expert qualifications and expert conclusions in this matter.
3. On August 3, 2023, Google submitted a response[2] to Plaintiffs' Motion for Preliminary Injunction, which included declarations[3,4,5] and documents that addressed issues raised in my initial report.
4. I was asked by Plaintiffs' counsel to review and submit this rebuttal declaration to address some of the issues raised in Google's response.
5. I reserve the right to amend, modify and rebuttal this declaration should new or additional information be made available to me.

I. ASSIGNMENT ON REBUTTAL

6. As noted above, I was asked to review and respond to some issues raised in Google's response. Specifically, I was asked to review and respond to the following:

[1] Declaration of Dr. Zubair Shafiq in Support of Plaintiffs' Motion for Preliminary Injunction, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431-VC ("Shafiq Declaration")

[2] Defendant Google LLC's Opposition to Plaintiffs' Motion for Preliminary Injunction and Motion to Dismiss, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431-VC, August 3, 2023

[3] Declaration of Dr. Georgios Zervas in Support of Defendant Google LLC's Opposition to Plaintiffs' Motion for Preliminary Injunction and Motion to Dismiss, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431-VC, August 3, 2023 ("Zervas Declaration").

[4] Declaration of Mr. Steve Ganem in Support of Defendant Google LLC's Opposition to Plaintiffs' Motion for Preliminary Injunction, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431-VC, August 2, 2023 ("Ganem Declaration").

[5] Declaration of Mr. Oscar Takabvirwa in Support of Defendant Google LLC's Opposition to Plaintiffs' Motion for Preliminary Injunction and Motion to Dismiss, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431-VC, August 3, 2023 ("Takabvirwa Declaration").

a. Google's role in the placement and configuration of Google's Advertising and Analytics products[6] on healthcare provider properties, as addressed in the Zervas and Ganem Declarations;

b. The technical operation of Google's Advertising and Analytics products including the collection of unique and persistent personal identifiers as well as their linking to Google account identifiers, as addressed in the Zervas and Ganem Declarations;

c. Google's ability to identify healthcare provider properties and classify website or app content containing sensitive health information, as addressed in the Zervas, Ganem, and Takabvirwa Declarations; and,

d. Google's use of sensitive health information for personalized advertising, as addressed in the Zervas, Ganem, and Takabvirwa Declarations.

II. MY CONCLUSIONS

7. Based upon my experience, expertise, review of the evidence, review of the testing data, and independent testing and analysis, I submit the following opinions and conclusions:

a. **Opinion # 1:** It is my expert opinion that Google plays a significant role in the placement and configuration of Google's Advertising and Analytics products on healthcare provider properties. For instance, Google Analytics source code is written solely by Google and provided to publishers to copy-paste on their properties, and Google employs various dark patterns to deceptively steer publishers and users into sharing personal data with Google. Peer-reviewed research and public statements of Google employees refute the arguments in the Zervas and Ganem Declarations.

b. **Opinion # 2:** It is my expert opinion that Google's Advertising and Analytics products routinely collect various personal user and device identifiers that Google regularly links to Google account identifiers and other types of

[6] "Google Advertising" products incudes Google Ads and Display Ads, and "Google Analytics" products refers collectively to Google Analytics 4, Universal Analytics, Google Analytics 360, and Google Analytics for Firebase.

personally identifiable information (PII). The Zervas and Ganem Declarations misrepresent the underlying technology, seem unaware of public evidence that clearly refutes their claims, and apply faulty testing and methodology that result in skewed results that do not accurately reflect real-world data transmissions.

c. **Opinion # 3:** It is my expert opinion that Google is not only highly capable of identifying healthcare provider properties and detecting sensitive health information but that it also actually does so on a routine basis in its various products. Public evidence and internal documents contradict the assertions in the Zervas, Ganem, and Takabvirwa Declarations.

d. **Opinion # 4:** It is my expert opinion that Google uses the information it collects from healthcare provider properties for personalized advertising, contradicting the assertions in the Zervas and Ganem Declarations. My replication of Dr. Zervas' methodology on this issue reveals that Google's policies and technical safeguards (if any) are inadequate. The Takabvirwa Declaration admits that Google indeed allows personalized advertising even for websites that it classifies as "sensitive", including healthcare provider websites.

III. OPINION # 1: GOOGLE'S ROLE IN PLACEMENT AND CONFIGURATION OF GOOGLE'S CODE ON PUBLISHER PROPERTIES

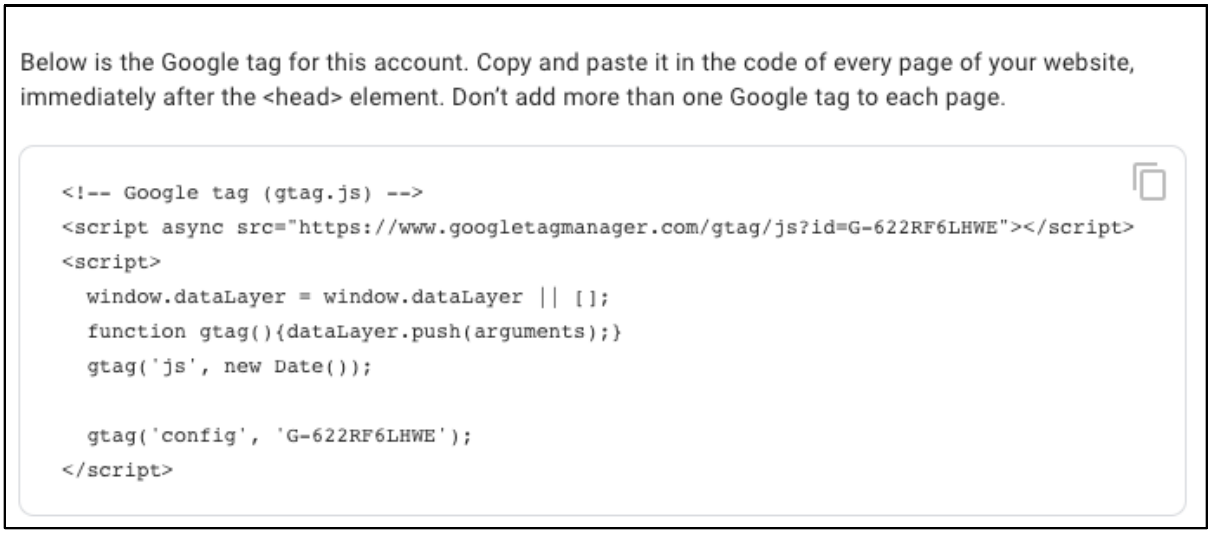
8. The Zervas and Ganem Declarations underplay Google's role in in the placement and configuration of Google's Advertising and Analytics Products on healthcare provider properties. They repeat the common misconception that "developers are responsible," thereby attempting to absolve Google of all and any responsibility.

a. Dr. Zervas states that "Developers—not third-party service providers—willingly choose to insert third-party code into their website or app to serve their needs" (Zervas Declaration ¶ 20) and that "developers are responsible for data they transmit to Google" (Zervas Declaration ¶ 85).

b. Mr. Ganem states that "Google does not have access to or control over the code of third-party websites, nor does Google affirmatively place Google Analytics code in third-party websites or on users' devices" (Ganem Declaration ¶ 6).

9. In saying this, Dr. Zervas and Mr. Ganem are significantly underplaying the access and control exerted by Google Analytics code on publisher websites.

a. It is noteworthy that Google asks publishers to integrate the Google code (i.e., "tag") as-is into their web pages. As shown in Figure 1, Google specifically instructs publishers to "copy and paste" the code "immediately after the <head> element". The publisher neither plays any part in writing the code nor can directly modify it. Thus, Google is mainly responsible for the content of the code it serves on publisher websites.



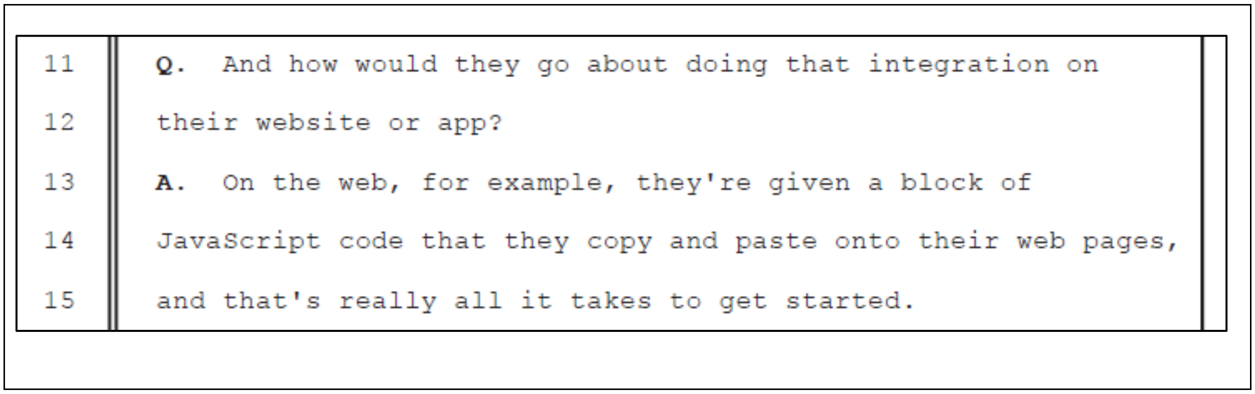
Below is the Google tag for this account. Copy and paste it in the code of every page of your website, immediately after the <head> element. Don't add more than one Google tag to each page.

```
<!-- Google tag (gtag.js) -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-622RF6LHWE"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'G-622RF6LHWE');
</script>
```

Figure 1: Installation instructions provided by Google to publishers on how to integrate Google Analytics code on their websites.

//
//
//

b. As shown in Figure 2, in another case against Google, *Calhoun v. Google, LLC*, Case No. 4:20-cv-5146-YGR,[7] Mr. Ganem publicly testified that Google supplied the code:



Q. And how would they go about doing that integration on their website or app?

A. On the web, for example, they're given a block of JavaScript code that they copy and paste onto their web pages, and that's really all it takes to get started.

Figure 2: Exhibit 1[8] at 156:11-15.

c. Dr. Zervas' assertion that Google cannot unilaterally remove its code from publishers' properties is wrong (Zervas Declaration ¶ 131). In fact, Google *can* control insertion or removal of its code from publishers' properties. Based on my experience in this field, there are many ways in which Google can stop its Google Analytics code from loading on healthcare provider websites if it wants to do so. For example, Google's server can include Cross-Origin Resource Sharing (CORS) headers[9] that specify which domains are allowed or disallowed from loading Google's source code. This technique is commonly used to prevent execution of code when requested by unauthorized domains. Modern web browsers, including Google's Chrome browser, implement CORS to block cross-domain JavaScript requests by default. As another example, Google can require authentication (e.g., using an access token) for its source code to execute. Yet another example, Google

[7] I submitted several expert reports and declarations in *Calhoun* on behalf of the plaintiffs. While, I was privy to confidential documents produced in that case, all of my analyses here, and information relied on, are based on publicly available information.

[8] Attached as **Exhibit 1** is a copy of the Oct. 24, 2022 Evidentiary Hearing held in the *Calhoun* case.

[9] Cross-Origin Resource Sharing (CORS) https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS

can also implement a referrer check — if the referrer does not match an approved list of sites, Google can deny the request to load its code.

10. It is also noteworthy that Google Analytics code on a webpage is not isolated within an "iframe".[10] Dr. Zervas explains that "developers who wish to use Google Analytics in their websites should add the analytics.js library ("the Google Analytics tag") "near the top of the <head> tag and before any other script or CSS tags" (Zervas Declaration ¶ 21). What Dr. Zervas fails to explain is that Google Analytics code has unrestricted access and control of the publisher webpage because it is not isolated in an iframe. This has critical implications. For instance, Google Analytics code can set and exfiltrate "first-party" cookies that are not impacted by the third-party cookie blocking. Additionally, Google Analytics code can directly manipulate the Document Object Model (DOM)[11] of the main page, which may include changing content, layout, and other structural elements. Google Analytics code can even capture user inputs. These are just a few examples of the implications that inclusion of such a script can exert if it is not properly isolated.

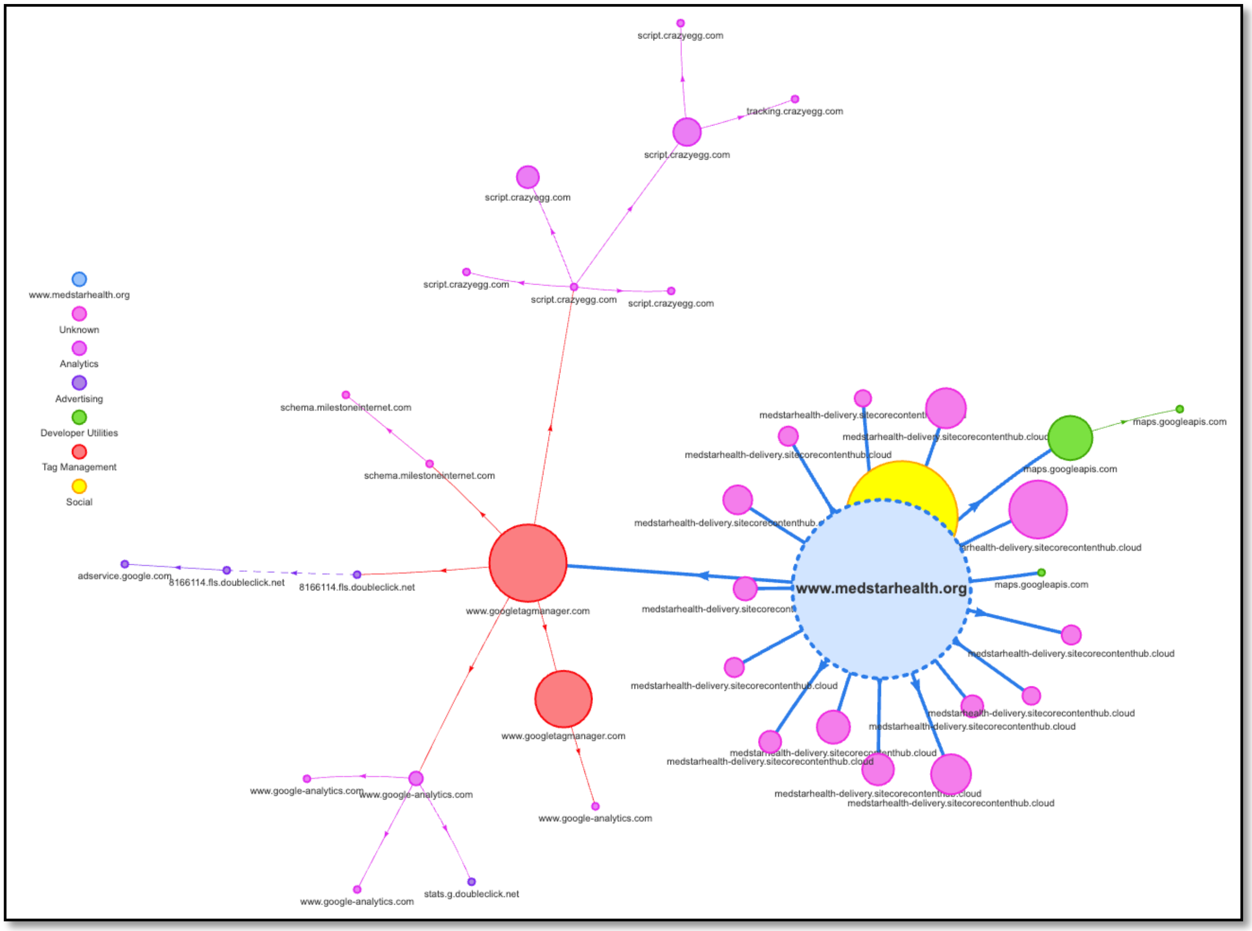
11. The conduct of Google's Advertising and Analytics products is particularly concerning when they further include additional parties. For example, Google Analytics (google-analytics.com) enables data collection by Google Ads (adservice.google.com) as well as Google Display Ads (doubleclick.net).

12. To illustrate this behavior, Figure 3(a) shows the network transmission graph for the "Abdominal Aneurysm Treatment | MedStar Health" webpage included in the Consolidated Complaint https://www.medstarhealth.org/services/abdominal-aneurysm-treatment generated using https://requestmap.webperf.tools. The nodes in the graph represent the individual server names involved in network transmissions. The edges in the graph are indicative of the specific network transmissions, attributing them to either the source code or the server responsible for initiating the transmissions. For the sake of clarity,

[10] <iframe>: The Inline Frame element https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe

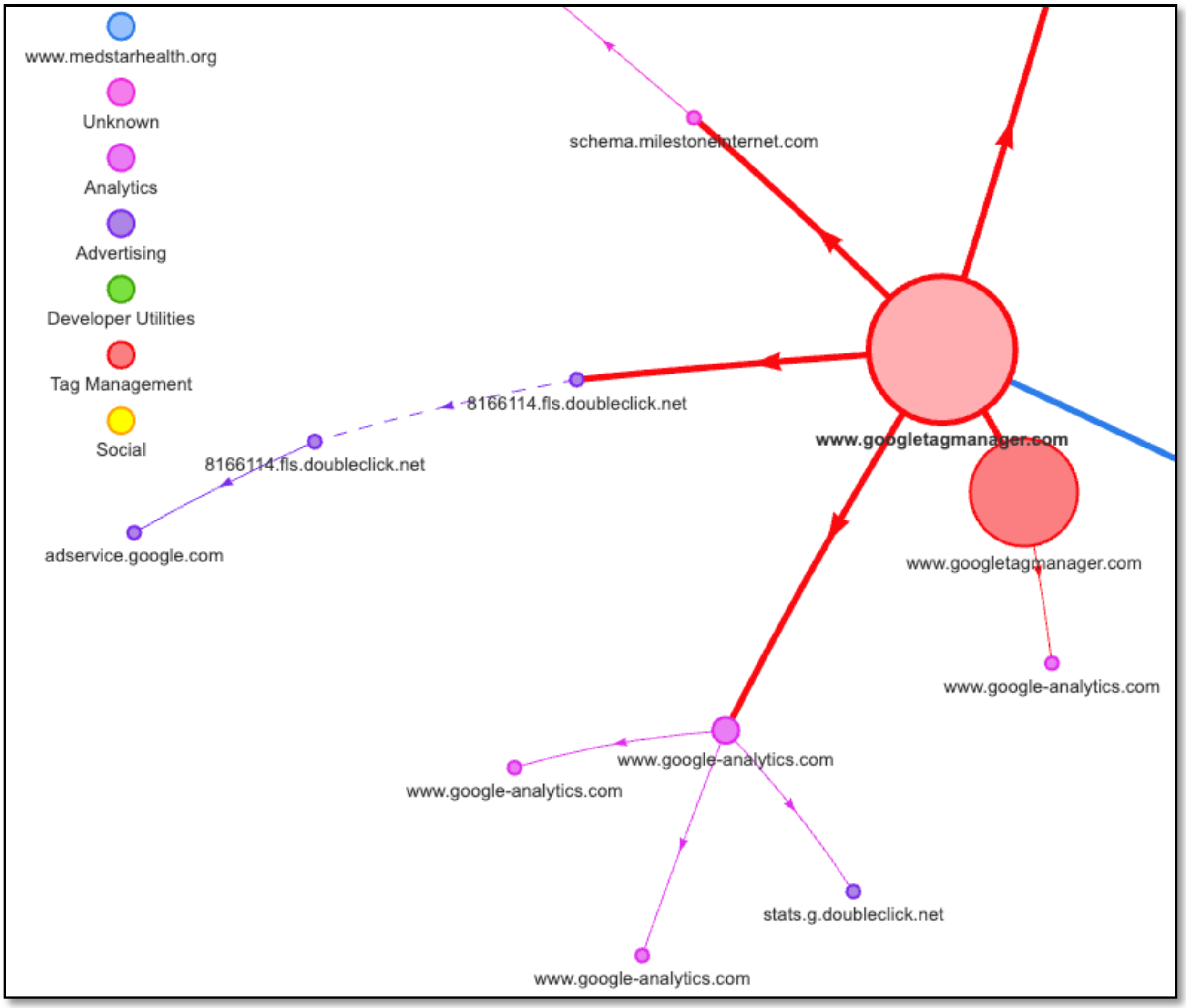
[11] DOM (Document Object Model) https://developer.mozilla.org/en-US/docs/Glossary/DOM

Figure 3(b) shows a zoomed-in version of Figure 3(a) focusing on Google-specific nodes in the graph. It is evident that the activation of third-party Google source code leads to the initiation of supplementary network transmissions directed towards additional Google third-party domains such as www.googletagmanager.com → www.google-analytics.com → stats.g.doubleclick.net.


script.crazyegg.com
tracking.crazyegg.com
script.crazyegg.com
script.crazyegg.com
script.crazyegg.com
script.crazyegg.com
script.crazyegg.com
www.medstarhealth.org
Unknown
Analytics
Advertising
Developer Utilities
Tag Management
Social
schema.milestoneinternet.com
schema.milestoneinternet.com
adservice.google.com
8166114.fls.doubleclick.net
8166114.fls.doubleclick.net
www.googletagmanager.com
www.googletagmanager.com
www.google-analytics.com
www.google-analytics.com
www.google-analytics.com
www.google-analytics.com
stats.g.doubleclick.net
medstarhealth-delivery.sitecorecontent
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
maps.googleapis.com
maps.googleapis.com
medstarhealth-delivery.sitecorecontenthub.
arhealth-delivery.sitecorecontenthub.cloud
www.medstarhealth.org
maps.googleapis.com
medstarhealth-delivery.sitecorecont
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud
medstarhealth-delivery.sitecorecontenthub.cloud

(a)

//
//
//



(b)

Figure 3: The network transmission graph for https://www.medstarhealth.org/services/abdominal-aneurysm-treatment. Note that Google's source code leads to the initiation of supplementary network transmissions directed towards additional Google third-parties.

//
//
//

13. These nested relationships emphasize the control that Google wields over data collection, which can be initiated simply by embedding a single Google script. While a publisher may anticipate transmissions to Google Analytics when including Google Analytics source code, it would not generally anticipate subsequent transmissions to additional Google domains at the 2nd level or beyond.[12]

14. It is imperative to note that Google designs and controls the technical infrastructure that facilitates the data collection and processing by its Advertising and Analytics products. The underlying mechanics, purposes, and utilization of the collected personal data are primarily under Google's purview. Google – at the very least – shares blame for its data collection, as Google architects and manages the system that enables this data collection, potentially extending beyond what publishers intend or understand.[13]

15. It is well-known in the scientific community that developers lack awareness regarding the third parties, such as Google Analytics, operating on their websites and the consequent data collection conduct. Specifically, in a recent peer-reviewed study[14] surveying about four hundred developers, Utz et al. reported "a widespread lack of awareness" among developers. The authors found that the publishers "either do not know or are uncertain of the true extent of data collection by the third party". The authors reported that the privacy policies of these third-party products, such as Google Analytics, "is insufficient to communicate its privacy risks". These findings demonstrate that Google indeed has access to and control over the code of websites where its third-party Advertising and Analytics products are integrated. The prevalent lack of awareness among developers concerning

[12] Ikram, M., Masood, R., Tyson, G., Kaafar, M. A., Loizon, N., & Ensafi, R. (2019, May). The chain of implicit trust: An analysis of the web third-party resources loading. In The World Wide Web Conference (pp. 2851-2857).

[13] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

[14] Utz, C., Amft, S., Degeling, M., Holz, T., Fahl, S., & Schaub, F. (2023). Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. Proceedings on Privacy Enhancing Technologies.

third-party data collection highlights that they are not in full control, thereby accentuating Google's significant role in the data collection on these websites.

16. Google is very much aware of the fact that publishers are unaware of the third parties, such as Google Analytics, and their data collection conduct on their properties. For example, Michael Kleber, a software engineer working on "privacy and tracking prevention in Chrome" explained at the 2019 Chrome Dev Summit that "If you are browsing the web, then even if you know where you are, what site you are visiting, ***you probably do not know all the third parties that are involved. And it is unreasonable to expect you to. What is more, if you are a developer building your own site, you might not know all of the third parties who could be pulled in when it runs***. This is like knowing your whole supply chain. Transitive dependencies are hard. And ***even if you know who they are you still might not know everything that they're doing***. (emphasis added)"[15]

17. Contrary to Mr. Ganem's assertion that "Developers […] choose whether and which data to collect, and whether and which data to provide to Google" (Ganem Declaration ¶ 9) and Dr. Zervas' conclusion that "developers are responsible" (Zervas Declaration ¶ 85), the reality of the situation has also been vividly exposed in peer-reviewed scientific research.

    a. Peer-reviewed research found that "[developers] often seem to not know or ignore the possibility that their visitors' personal data could be collected for other purposes, or simply trust the third-party service to not collect data or to employ adequate privacy protection."[16] This conclusion elucidates the fact that developers' choices are not entirely conscious or informed. Instead, it underscores Google's significant influence in data collection, contradicting Mr. Ganem's and Dr. Zervas' attempts to downplay Google's part in this process.

    b. Google is known to strategically employ ***dark patterns*** to steer publishers towards decisions that adversely affect consumer privacy. These tactics range from

[15] Protecting users on a thriving web (Chrome Dev Summit 2019) https://www.youtube.com/watch?v=WnCKlNE52tc

[16] *Id*. at 9

configuring privacy-unfriendly defaults, obscuring privacy-friendly options, utilizing visual manipulation, instituting false hierarchy, and incorporating nagging dark patterns in sample code. In a recent peer-reviewed study, Tahaei et al. found that Google employs various dark patterns to steer developers into making privacy-unfriendly "choices" – even though privacy-friendlier options do exist but are often hidden or obscured by dark patterns.[17]

i. The authors found that Google uses "toying with emotion by hinting that developers get higher revenue or better analytics by sharing more data".

ii. The authors found that Google uses "aesthetic manipulation in the content categories UI by having a blue toggle represent blocked items and a grey one for allowed items".

iii. The authors found that "regulation defaults are set to off, data collection is not limited, personalized ads are allowed, user consent is by default set to true in sample code, and content categories are all set to on."

iv. The authors found that Google "uses false hierarchy by making the first option on the consent popup builder not include a 'Do not consent' option, while the second nearly-identical choice does".

v. The authors found that Google's sample code "continues to ask for user consent even if they decline it, which is a clear example of nagging behavior."

vi. The authors found that Google's sample code "notif[ies] the user about using location without giving them any options to refuse, or providing consent popups that do not have a 'I do not consent' button."

18. In litigation related to Google's collection and use of consumers' location data, plaintiffs' expert Colin Gray, Ph.D. concluded that the user interfaces of Google services "contain[ed]

[17] Tahaei, M., & Vaniea, K. (2021, May). "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In 2021 CHI Conference on Human Factors in Computing Systems.

specific dark patterns that hide important complexity from end users and are designed in a manner that would lead users to think they are managing the totality of location tracking when they are not." *State of Arizona v. Google LLC*, No. CV2020-006219 (Maricopa Cnty., AZ), Gray Dark Patterns Report, **Exhibit 2** at 2. Dr. Gray summarized several documents produced by Google, detailing the deceptive nature of user controls like WAA and sWAA:

> David Monsees, whom I understand is the product manager for WAA at Google, states in an email regarding WAA: *"In no way am I saying the names are great, they do cause a bit of confusion (e.g., how do you tell a user how to turn on sWAA). WAA would be great if it was called something like, "stuff you do with Google", but there is a lot of blur."* (GOOG-GLAZ-00312069). Monsees similarly expressed concerns regarding the information stored (as opposed to simply collected) through WAA. (GOOG-GLAZ-00107030) at 30 ("The general takeaway is that no one know [sic] what is currently written to Footprints[] or why."). Even with WAA off, an email from Google employee Chris Ruemmler indicates that *"The WAA and other controls imply we don't log the data, but obviously we do. We need to change the description to indicate even with the [WAA] control off, Google retains this data and uses it for X purposes"* (GOOG-GLAZ-00312075 at 075). In this same email, Ruemmler indicates that the wording used to describe the activity controls is *"very deceptive,"* and suggests that Google perform studies *"to see what customers think is happening with their data when they disable these controls […] and know if what is written is being properly interpreted by our users. I have a fear it most likely is not."* (GOOG-GLAZ-00312075 at 075).

Gray Dark Patterns Report at 20.

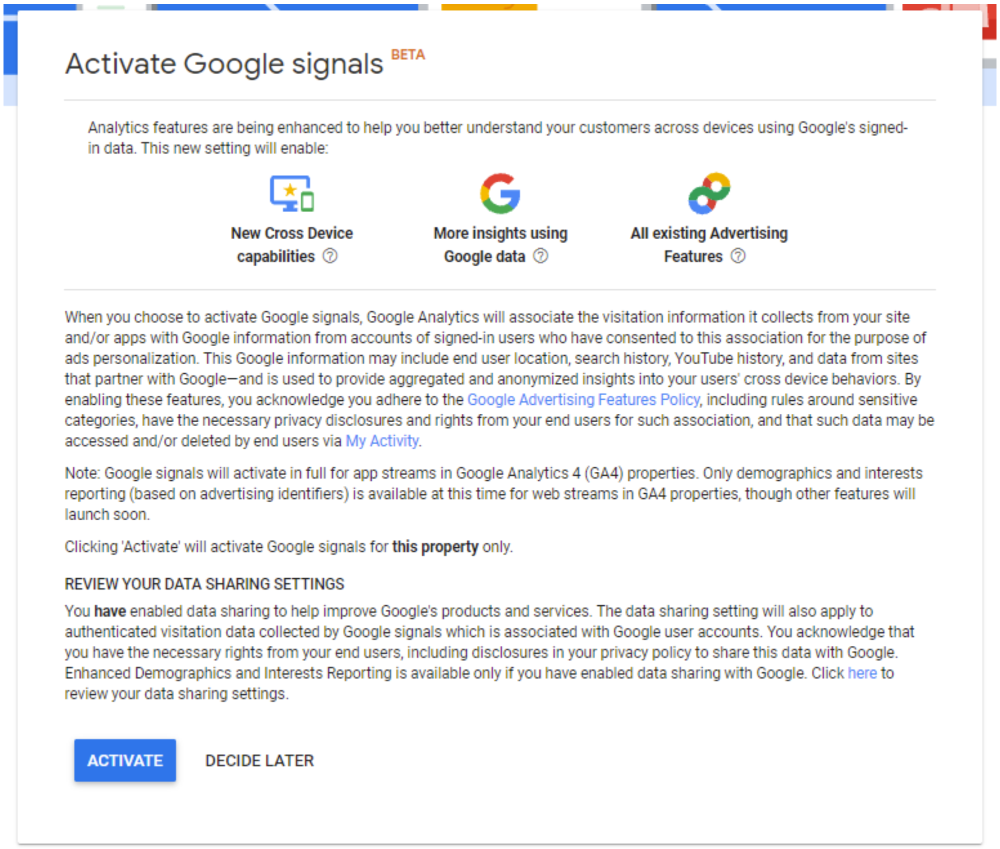
19. Mr. Ganem states that "If the developer has enabled Google Signals and a Google Account owner has turned on their WAA, sWAA, GAP, and NAC settings, the user's data may be connected to their Google account in what is known as 'GAIA space'" (Ganem Declaration ¶ 42). As I introduced above in the developer context, and discuss more so below in the user context, Google employs dark patterns that manipulate both developers and users.

   a. Google Signals: Google employs various dark patterns that interfere with developers' ability to not enable Google Signals on its properties.[18] As an example, Figure 4 shows how Google highlights privacy unfriendly "ACTIVATE" option in blue and makes "DECIDE LATER" much less noticeable in contrast. Also note how

[18] *Id.*

Google hints to developers that they get “more insights” and “new […] capabilities” if they enable Google Signals.

b. Google Account Settings: Google employs various dark patterns that interfere with users’ ability to disable (or not enable) WAA and sWAA as well as GAP and NAC settings. These include but are not limited to privacy-unfriendly default settings, hiding privacy-friendly choices, giving users an illusion of control, employing misleading wording, and providing choice architectures where choosing privacy-friendly option requires more effort. As an example, Figures 5 and 6 show evidence that Google employed privacy-unfriendly defaults.



Activate Google signals BETA

Analytics features are being enhanced to help you better understand your customers across devices using Google's signed-in data. This new setting will enable:

New Cross Device capabilities
More insights using Google data
All existing Advertising Features

When you choose to activate Google signals, Google Analytics will associate the visitation information it collects from your site and/or apps with Google information from accounts of signed-in users who have consented to this association for the purpose of ads personalization. This Google information may include end user location, search history, YouTube history, and data from sites that partner with Google—and is used to provide aggregated and anonymized insights into your users' cross device behaviors. By enabling these features, you acknowledge you adhere to the Google Advertising Features Policy, including rules around sensitive categories, have the necessary privacy disclosures and rights from your end users for such association, and that such data may be accessed and/or deleted by end users via My Activity.

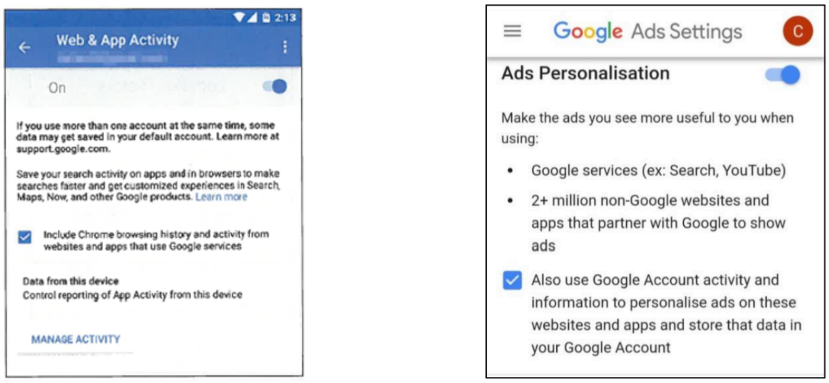
Note: Google signals will activate in full for app streams in Google Analytics 4 (GA4) properties. Only demographics and interests reporting (based on advertising identifiers) is available at this time for web streams in GA4 properties, though other features will launch soon.

Clicking 'Activate' will activate Google signals for **this property** only.

REVIEW YOUR DATA SHARING SETTINGS

You **have** enabled data sharing to help improve Google's products and services. The data sharing setting will also apply to authenticated visitation data collected by Google signals which is associated with Google user accounts. You acknowledge that you have the necessary rights from your end users, including disclosures in your privacy policy to share this data with Google. Enhanced Demographics and Interests Reporting is available only if you have enabled data sharing with Google. Click here to review your data sharing settings.

Figure 4: Screenshot of the Google Signals activation screen.



Web & App Activity

On

If you use more than one account at the same time, some data may get saved in your default account. Learn more at support.google.com.

Save your search activity on apps and in browsers to make searches faster and get customized experiences in Search, Maps, Now, and other Google products. Learn more

☑ Include Chrome browsing history and activity from websites and apps that use Google services

Data from this device
Control reporting of App Activity from this device

MANAGE ACTIVITY

Google Ads Settings

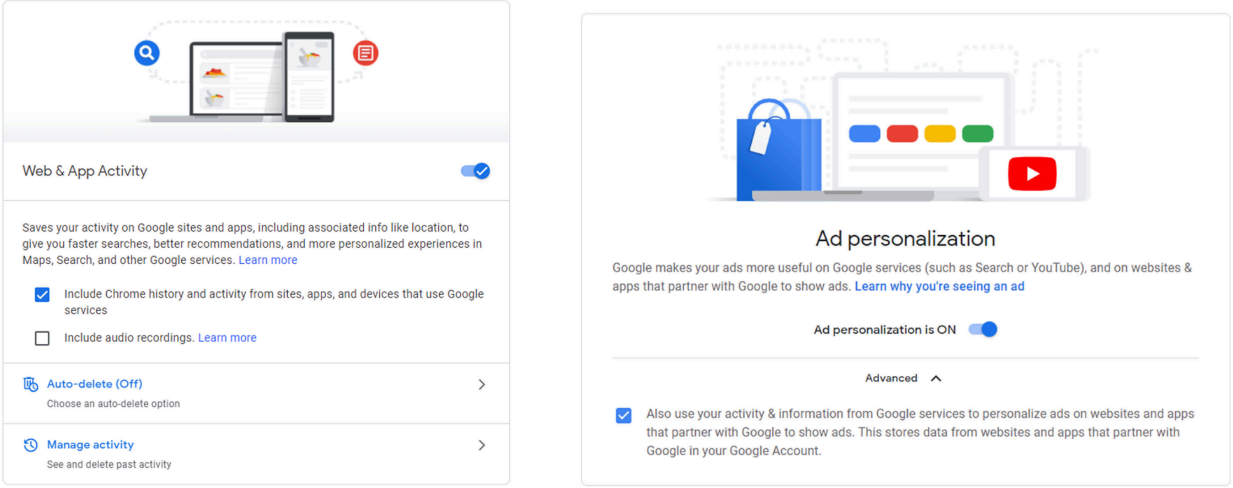
Ads Personalisation

Make the ads you see more useful to you when using:

- Google services (ex: Search, YouTube)
- 2+ million non-Google websites and apps that partner with Google to show ads

☑ Also use Google Account activity and information to personalise ads on these websites and apps and store that data in your Google Account

Figure 5: Screenshots of WAA (top-left), sWAA (bottom-left), GAP (top-right), and NAC (bottom-right) settings as documented in prior reporting of the Norwegian Consumer Council[19] and Australian Competition & Consumer Commission[20].



Web & App Activity

Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

☑ Include Chrome history and activity from sites, apps, and devices that use Google services

☐ Include audio recordings. Learn more

Auto-delete (Off)
Choose an auto-delete option

Manage activity
See and delete past activity

Ad personalization

Google makes your ads more useful on Google services (such as Search or YouTube), and on websites & apps that partner with Google to show ads. Learn why you're seeing an ad

Ad personalization is ON

Advanced

☑ Also use your activity & information from Google services to personalize ads on websites and apps that partner with Google to show ads. This stores data from websites and apps that partner with Google in your Google Account.

Figure 6: Screenshots of WAA (top-left), sWAA (bottom-left), GAP (top-right), and NAC (bottom-right) settings as documented in Mr. Ganem's declaration in a related matter.[21]

IV. OPINION # 2: COLLECTION OF UNIQUE AND PERSISTENT PERSONAL IDENTIFIERS BY GOOGLE'S ADVERTISING AND ANALYTICS PRODUCTS

20. The Zervas and Ganem Declarations misconstrue the underlying technical details as to whether and how the information collected by Google's Advertising and Analytics products includes unique and persistent identifiers. Their assertions about Google's policies against

[19] *Id.*

[20] Google LLC to pay $60 million for misleading representations https://www.accc.gov.au/media-release/google-llc-to-pay-60-million-for-misleading-representations

[21] *Calhoun v. Google*, Case 5:20-cv-5146-LHK-SVK; Document 430-9 (pages 16--17). Attached as **Exhibit 3.**

linking these identifiers to Google account identifiers and other types of PII is contradicted by public information.

21. In Sections III.C and III.D of his report, Dr. Zervas concludes that "Plaintiffs incorrectly allege that Google associates the data it collects from health-related web properties to other information it has collected about users" (Zervas Declaration ¶ 16). In these sections, Dr. Zervas relies upon declarations from Google employees to make a number of assertions that are either false or misleading. For example, Mr. Ganem asserts that "If any of these controls are off, only pseudonymous data is collected; the data is not joined to the user's Google account and is not stored in 'GAIA space'" (Ganem Declaration ¶ 42).

22. As described in more detail below, I disagree with these assertions.

23. To help the Court understand why, it is important to first discuss and understand the identifiers that are relevant to my analysis. I lay out those identifiers[22], and a brief description, below:

    a. GAIA ID: Based on publicly available information, including publicly filed court documents, it is my understanding that the GAIA ID identifies Google account holders and is transmitted when a user is signed-in to their Google account. Based on my general experience reviewing, analyzing and testing data transmissions, the GAIA ID (*e.g.* the value) is stored within many different types of cookies that are sent to Google, including cookies set to the Google Ads domain, google.com, and Google display ads, doubleclick.net. These cookies include SID, HSID, SSID, OSID (google.com) and DSID (doubleclick.net). The cookies allow Google to track users across different web-properties and, because the GAIA ID is tied to a specific Google account (*e.g.,* an individual's email address), the identifier is capable of identifying an individual.

[22] I separately discuss IP address, user agent, and other attributes that can be used by Google for fingerprinting (also known as *probabilistic matching*).

b. Biscotti ID (IDE): The Biscotti ID identifies signed-out Google account holders. The Biscotti ID is usually stored in IDE cookies, which are sent to Google Display Ads (to doubleclick.net). This cookie, with a lifetime of 13 months, tracks users across different web properties and is associated with the specific device-browser.

c. Zwieback ID (NID): The Zwieback ID identifies signed-out Google account holders. The Zwieback ID is usually stored in NID cookies, which are sent to Google Ads (to google.com). This cookie, with a lifetime of 6 months, tracks users across different web properties and is associated with the specific device-browser.

d. Client ID: The Client ID is the identifier that Google Analytics uses to identify a site's visitors. It is stored in _ga cookie, with a lifetime of 2 years, and is sent to Google via the "cid" URL query parameter. A user cannot simply reset their Client ID by removing third-party cookies because Google's source code ghost writes[23] it in a "first-party" cookie. This Client ID is shared with other third-party domains.

e. AdID: Google Advertising ID is the identifier that Google uses to identify a mobile specific device across different apps. It does not expire unless it is affirmatively reset.

f. IDFA: Identifier for Advertising (IDFA) is the identifier that iOS devices use to identify specific iOS mobile devices across different apps. It does not expire unless it is affirmatively reset.

24. It is my understanding that Google has claimed that some of these identifiers, except for GAIA, are "pseudonymous", *i.e.,* they can be used to identify or track an individual but do

[23] "Ghost writes" means that cookies are set on behalf of a party (e.g., the website the user is currently visiting) but are actually written by a different entity (e.g., a third-party script).

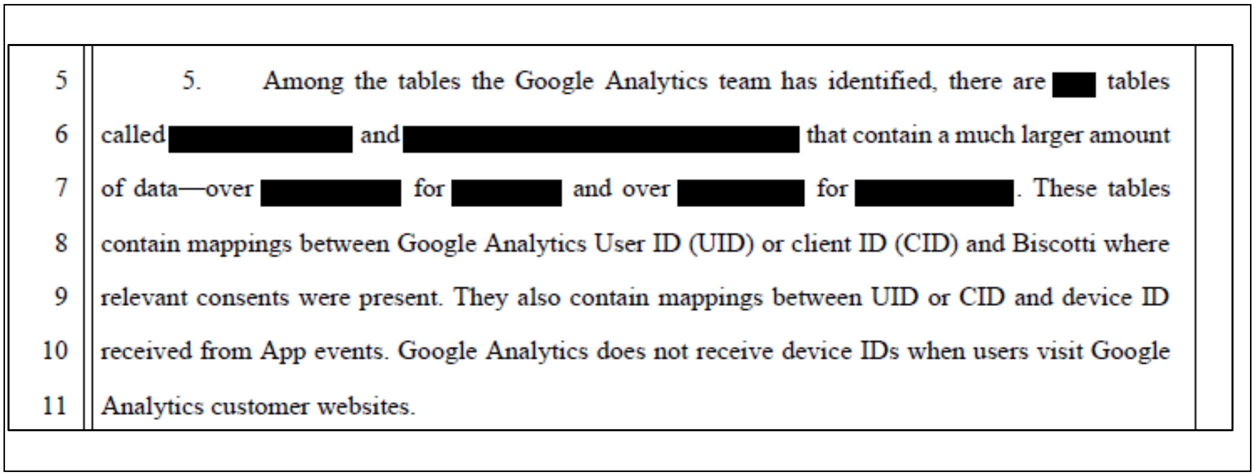
not directly contain a person's name or other forms of PII. But this statement is not consistent with my research, understanding, and analysis of how Google's systems work.[24]

25. Google ***can and does*** link these "pseudonymous" identifiers with GAIA ID and other forms of PII. Specifically, Google maps Biscotti ID, Zwieback ID, Google Analytics Client ID, and mobile advertising IDs (like AdID and IDFA) to identifiers that are directly linked to individuals, like GAIA ID. There is abundant evidence that isolation of "pseudonymous" identifiers from "GAIA space" is untrue – the "pseudonymous" (or non-GAIA) data collected by Google is indeed linked to the "GAIA space." I provide further background and explanation on this below.

26. In ¶ 40 of his declaration, Dr. Zervas states that "the value of the _ga cookie is the Client ID—a randomly generated pseudonymous identifier that allows Google Analytics to record browsing activities that take place only on this first-party website within the same browser. In other words, the Client ID is unique to each website, and cannot be used to track users across the web." In support of this, Dr. Zervas cites to the Ganem Declaration ¶ 34 and his Appendix C. Dr. Zervas' Appendix C does not contain any reference to Google internal information that he was provided to support this conclusion.

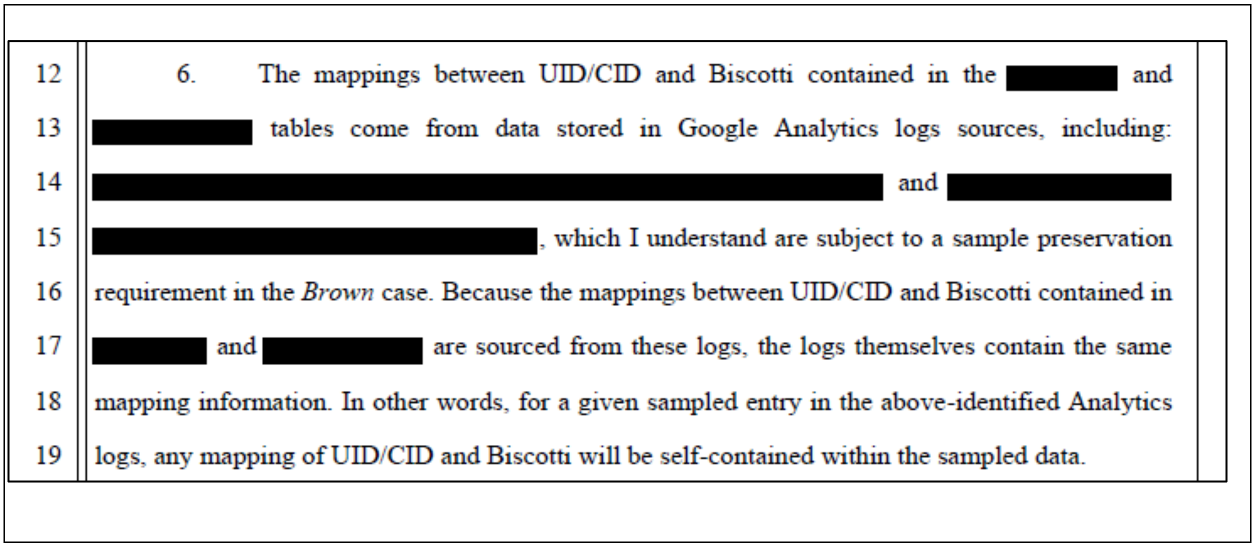
27. In contrast to Dr. Zervas' above statement, which appears to rely solely on the Ganem Declaration, in *Calhoun v. Google* Google filed a motion on October 27, 2022 that requested relief from a preservation order. *Calhoun,* Dkt. 898.In support of the motion, Google submitted the Declaration of Srilakshmi Pothana, who stated that Google Analytics maintains "tables [that] contain mappings between Google Analytics User ID (UID) or client ID (CID) and Biscotti" as well as "mapping between UID or CID and device ID when received from App Events." *Calhoun* Dkt. 898-9, ¶ 5 (attached as **Exhibit 4).**

[24] It is also my understanding that this statement is not consistent with the HIPAA Deidentification Rule at 45 C.F.R. § 164.514 and Cal. Civ. Code § 1798.140(v)(1); (aj), which, respectively, expressly define "individually identifiable" and "personal information" to include IP addresses and device identifiers, such as cookies.



5. Among the tables the Google Analytics team has identified, there are [redacted] tables called [redacted] and [redacted] that contain a much larger amount of data—over [redacted] for [redacted] and over [redacted] for [redacted]. These tables contain mappings between Google Analytics User ID (UID) or client ID (CID) and Biscotti where relevant consents were present. They also contain mappings between UID or CID and device ID received from App events. Google Analytics does not receive device IDs when users visit Google Analytics customer websites.

28. Ms. Pothana also stated that:

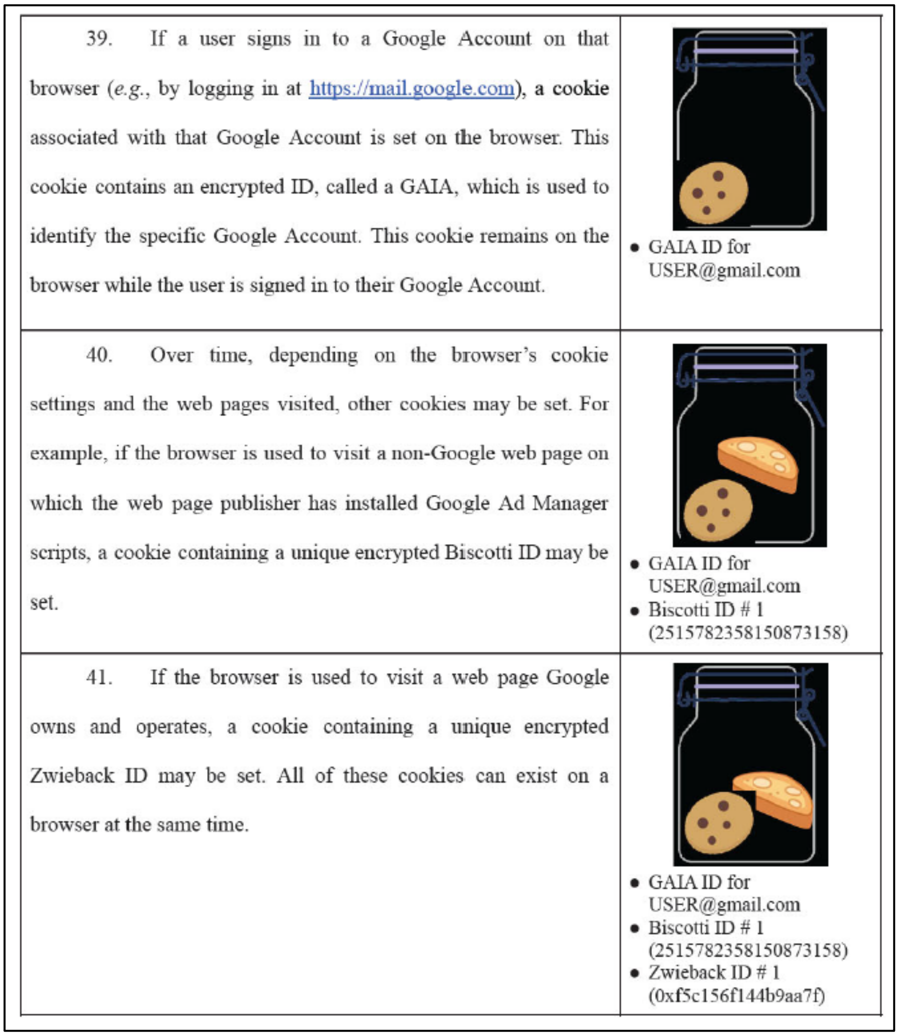


6. The mappings between UID/CID and Biscotti contained in the [redacted] and [redacted] tables come from data stored in Google Analytics logs sources, including: [redacted] and [redacted], which I understand are subject to a sample preservation requirement in the *Brown* case. Because the mappings between UID/CID and Biscotti contained in [redacted] and [redacted] are sourced from these logs, the logs themselves contain the same mapping information. In other words, for a given sampled entry in the above-identified Analytics logs, any mapping of UID/CID and Biscotti will be self-contained within the sampled data.

29. It is my understanding that the Court in *Calhoun* granted Google's motion on April 4, 2023, repeating Ms. Pothana's statement that Google keeps "tables [that] contain mapping between Google Analytics User ID (UID) or client ID (CID) and Biscotti." *Calhoun* Dkt. 1008, Order Relieving Google of Certain Preservation Obligations, at 8 (attached as **Exhibit 5).**

30. Google has also submitted evidence in another case, *Brown v. Google*, Case No. 4:20-cv-03664-YGR, which appears to contradict the statements that are being made in this action. For example, in *Brown*, Google submitted documents that state:

a. Google simultaneously stores the GAIA ID and the Biscotti ID in the browser's cookie jar in the DSID cookie and the IDE cookie, respectively. Google collects both GAIA and Biscotti IDs in each transmission to Google (i.e., doubleclick.net), and hence can map Biscotti to GAIA or vice-versa for signed-in Google account holders. Google's expert illustrated this using the following diagram in a related matter (*Brown*, Dkt. 666-21 at 21, ¶¶ 39-41, attached as **<u>Exhibit 6</u>**). Google explained that a user's cookie jar could include GAIA, Biscotti, and Zwieback. See Figure 7.



39. If a user signs in to a Google Account on that browser (*e.g.*, by logging in at https://mail.google.com), a cookie associated with that Google Account is set on the browser. This cookie contains an encrypted ID, called a GAIA, which is used to identify the specific Google Account. This cookie remains on the browser while the user is signed in to their Google Account.	● GAIA ID for USER@gmail.com
40. Over time, depending on the browser's cookie settings and the web pages visited, other cookies may be set. For example, if the browser is used to visit a non-Google web page on which the web page publisher has installed Google Ad Manager scripts, a cookie containing a unique encrypted Biscotti ID may be set.	● GAIA ID for USER@gmail.com ● Biscotti ID # 1 (2515782358150873158)
41. If the browser is used to visit a web page Google owns and operates, a cookie containing a unique encrypted Zwieback ID may be set. All of these cookies can exist on a browser at the same time.	● GAIA ID for USER@gmail.com ● Biscotti ID # 1 (2515782358150873158) ● Zwieback ID # 1 (0xf5c156f144b9aa7f)

Figure 7: Google's expert explains that the cookie jar includes GAIA, Biscotti, and Zwieback identifiers at the same time.

b. "Conversions are measured through mapping a GAIA ID to a Biscotti ID. GOOG-CABR-03662096 at -100" (*Brown*, Dkt. 666-21 at 43, ¶88).

c. Google employs a "User ID Relation Graph… [which] relates user-id with other identifiers (device-id physical, aaid, idfa, phone, email)" (GOOG-CABR-04782308 at -309)" (*Brown*, Dkt. 643-8 at 110, ¶ 253, attached as **<u>Exhibit 7</u>**).

d. Google employs a "User Trust Graph". Specifically, the following quotes from Google's internal documents show that Google links "pseudonymous" identifiers with GAIA ID or other forms of PII (*Brown*, Dkt. 643-8 at 111, ¶ 254).

   i. "The user id's are nodes of the graph. Aggregated information about user activity and information about the user is anchored on the node as an attribute" (GOOG-CABR-04782100 at -101).

   ii. "AdSpam team already has event level logs access across id spaces" (GOOG-CABR-04732430 at -433)".

31. In *Calhoun*, I submitted an expert report on November 14, 2022 that summarized my findings and analysis of a production of documents that Google made on October 28, 2022. In my report, I explain that "my analysis of Google's production … shows that Google commingles signed-in and signed-out information in various … columns," including "'trifecta' proto files, i.e. files that simultaneously store GAIA, Biscotti, and Zwieback IDs and associated information (e.g. age, ethnicity, race, precise coordinates, credit card data, and other identifiers such as device ID)."[25] I later explained that one of the protos contained these three identifiers plus fields with demographic, location, financial information and other identifiers including age, gender, race, ethnicity, income, children, education, precise geo-coordinates, areas of interest, shipping address, credit card information, household income, PPID, Device ID, First Party User ID, Buyside publisher ID, Publisher User ID,

[25] *Calhoun* Dkt. 920-6, Report of Zubair Shafiq In Support of Plaintiffs' Sur-reply in Further Opposition to Google's Motion for Summary Judgment, at 2, ¶ 6. Attached as **<u>Exhibit 8.</u>**

DUSI, and YouTube Visitor ID.[26] I then explained that Google also maintains (1) "numerous proto files that contain GAIA ID along with Biscotti ID or Zwieback ID;" (2) "proto files … that contain Biscotti ID and Zwieback ID;" (3) "proto files that contain GAIA, Biscotti, or Zwieback as well as other identifier[s] that can be used to bridge GAIA, Biscotti, and Zwieback ID spaces" including "device IDs such as Android ID (ADID) and iOS IDFA, DUSI."[27]

32. The above evidence from *Calhoun* and *Brown* undermine the statements made by Dr. Zervas and Mr. Ganem that some "pseudonymous" identifiers can never be identifiable information. Such conclusion is not true because information in *Calhoun* and *Brown* demonstrate that Google does in practice associate "pseudonymous" identifiers to individual identifiers.

33. Dr. Zervas analyzes transmissions of "first-party" and third-party cookies to Google (Zervas Declaration ¶¶ 28—32). But his analysis relies on a flawed methodology and misrepresents how cookies are set and transmitted by Google's source code to Google's servers.

34. Dr. Zervas states that he "captured transmissions and analyzed homepages of the 11 healthcare providers' domains studied in the Smith Declaration." (Zervas Declaration ¶ 31). He then provides Appendix C for a detailed explanation of how of how he performed his testing.

35. In Appendix C, Dr. Zervas states that, to begin each test, he did the following: "open the selected browser (either Chrome or Firefox, as described above), clear all browsing data (e.g. cookies and cache), and select the setting or extension of interest." (Zervas Declaration Appendix C; ¶ 12(a)).

36. This testing is flawed because Dr. Zervas' only tested the homepages of various healthcare provider properties. He failed to include any internal subpages that would have included

[26] *Id*. at ¶ 18.

[27] *Id*. at ¶¶ 19-21.

information about communications beyond just the home page domain. A typical user would not just browse the home page[28] of a healthcare provider but also access subpages whose URL would contain more detailed information pertaining to a doctor, condition, treatment, or patient portal login. In looking only at the homepages, Dr. Zervas' testing is intentionally skewed to eliminate any evidence of transmissions of content URLs (i.e., URLs that contain specific information about what a user may be viewing or doing), and eliminates any analysis of what happens when a user is in a patient portal.

37. Dr. Zervas' testing methodology is also flawed because it is a "stateless" crawl of the healthcare provider properties, meaning that Dr. Zervas commenced the test with a browser that had been cleared of any previous activity – devoid of browsing data and cookies – thereby simulating an unrealistic environment. This "stateless" approach does not accurately represent how consumers experience browser usage in the real world. A typical user's browsing session retains information, including cookies, which would facilitate transmissions to third parties like Google Ads assuming the user had visited Google.com previously.

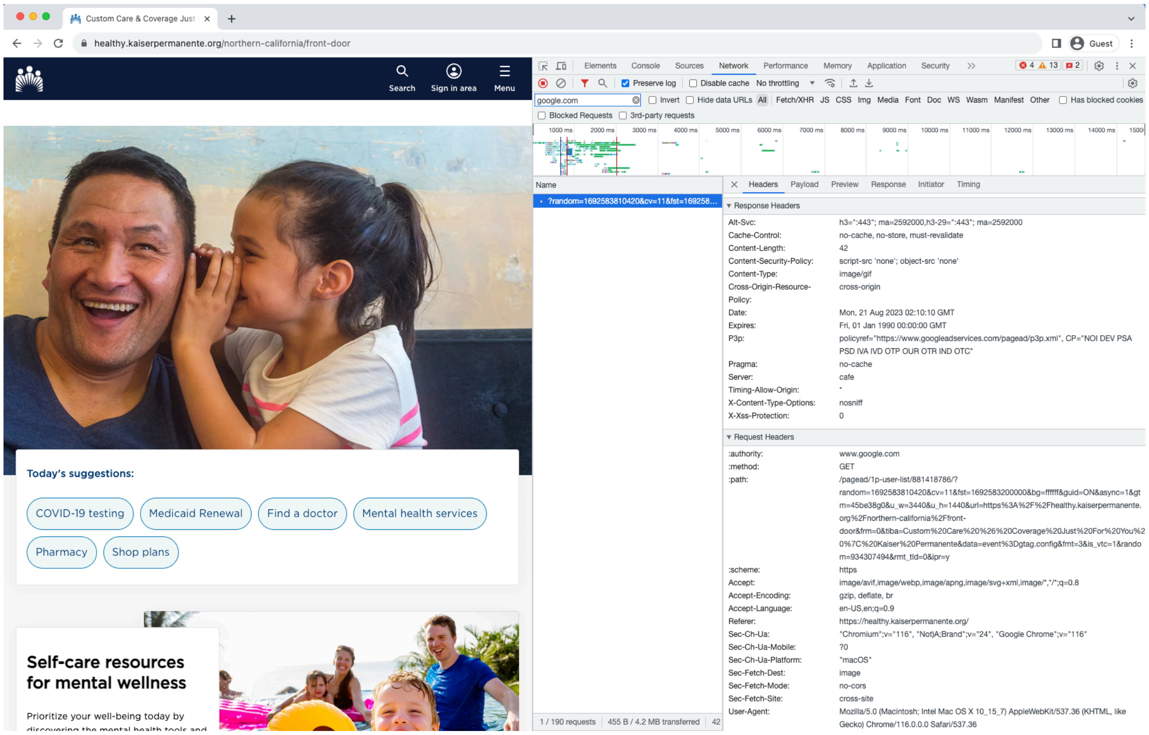
38. Peer-reviewed research[29] showed that an average user encounters Google "on average every 1.11 hours". The authors go on to explain that "to fully prevent the largest company in our dataset from being involved in tracking practices, a user should delete the cookies after every single browsing hour, which is obviously not realistic." In other words, an average user visiting a healthcare property, such as those tested by Dr. Zervas, would already have Google cookies set in their browser within an hour of browsing on average.

[28] Aqeel, W., Chandrasekaran, B., Feldmann, A., & Maggs, B. M. (2020, October). On landing and internal web pages: The strange case of jekyll and hyde in web performance measurement. In Proceedings of the ACM Internet Measurement Conference (pp. 680-695).

[29] Dambra, S., Sanchez-Rola, I., Bilge, L., & Balzarotti, D. (2022). When Sally Met Trackers: Web Tracking From the Users' Perspective. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 2189-2206).

39. While a “stateless” test might hold value for certain types of analysis, it lacks credibility with regard to the examination network transmission for a real user’s browser to third-parties like Google.

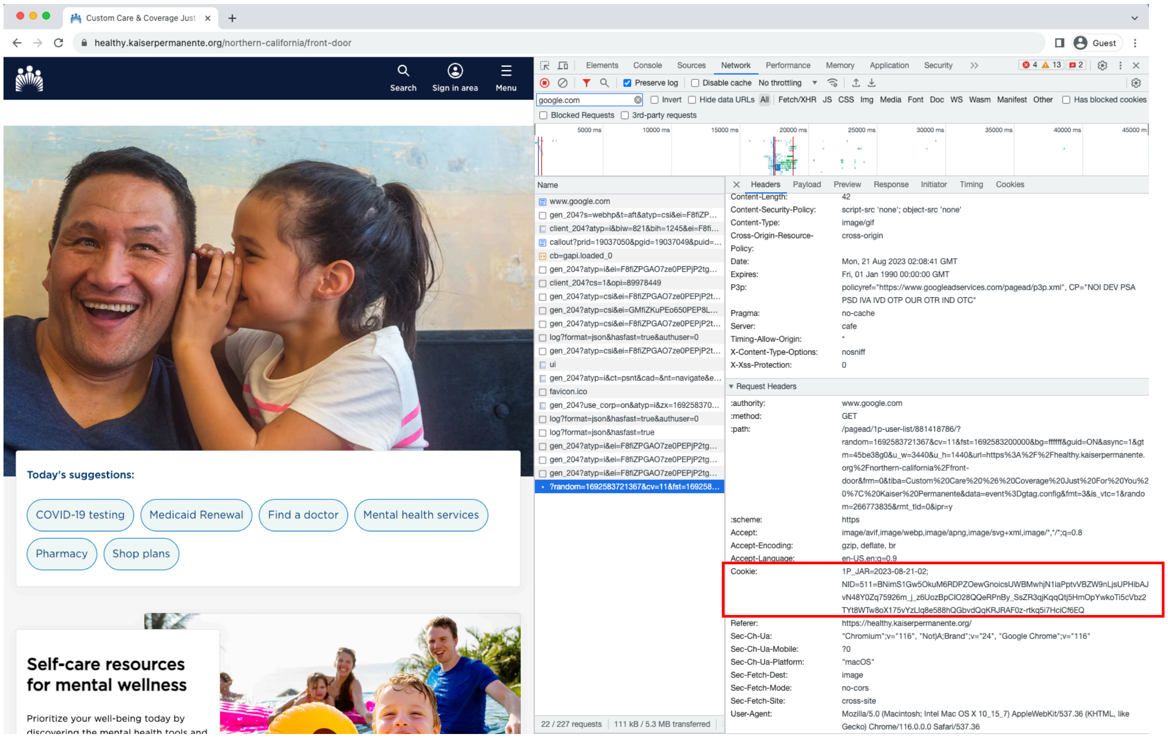
40. To drive this point home, I repeat “stateless” and “stateful” crawls[30] of the first site (https://healthy.kaiserpermanente.org) used in Dr. Zervas’ and Mr. Smith’s tests. (Zervas Declaration ¶ 31). In the “stateless” crawl, I directly visit the Kaiser Permanente site in a fresh browser that does not contain any previous cookies. In the “stateful” crawl, I first visit www.google.com in a fresh browser that does not contain any previous cookies and then visit the Kaiser Permanente site while preserving the cookies set in the browser in the first visit. Figure 8 highlights the difference in cookie transmissions to Google.com. Note that there are no cookie transmissions to Google.com in the “stateless” crawl, as Dr. Zervas shows in his analysis. However, there are cookie transmissions to Google.com in the “stateful” crawl, including the NID Zwieback cookie that Dr. Zervas’ analysis omits.



```
?random=1692583810420&cv=11&fst=169258...

▼ Response Headers
Alt-Svc:                        h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control:                  no-cache, no-store, must-revalidate
Content-Length:                 42
Content-Security-Policy:        script-src 'none'; object-src 'none'
Content-Type:                   image/gif
Cross-Origin-Resource-          cross-origin
Policy:
Date:                           Mon, 21 Aug 2023 02:10:10 GMT
Expires:                        Fri, 01 Jan 1990 00:00:00 GMT
P3p:                            policyref="https://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA
                                PSD IVA IVD OTP OUR OTR IND OTC"
Pragma:                         no-cache
Server:                         cafe
Timing-Allow-Origin:            *
X-Content-Type-Options:         nosniff
X-Xss-Protection:               0

▼ Request Headers
:authority:                     www.google.com
:method:                        GET
:path:                          /pagead/1p-user-list/881418786/?
                                random=1692583810420&cv=11&fst=1692583200000&bg=ffffff&guid=ON&async=1&gt
                                m=45be38g0&u_w=3440&u_h=1440&url=https%3A%2F%2Fhealthy.kaiserpermanente.
                                org%2Fnorthern-california%2Ffront-
                                door&frm=0&tiba=Custom%20Care%20%26%20Coverage%20Just%20For%20You%2
                                0%7C%20Kaiser%20Permanente&data=event%3Dgtag.config&fmt=3&is_vtc=1&rando
                                m=934307494&rmt_tld=0&ipr=y
:scheme:                        https
Accept:                         image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:                gzip, deflate, br
Accept-Language:                en-US,en;q=0.9
Referer:                        https://healthy.kaiserpermanente.org/
Sec-Ch-Ua:                      "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Sec-Ch-Ua-Mobile:               ?0
Sec-Ch-Ua-Platform:             "macOS"
Sec-Fetch-Dest:                 image
Sec-Fetch-Mode:                 no-cors
Sec-Fetch-Site:                 cross-site
User-Agent:                     Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
                                Gecko) Chrome/116.0.0.0 Safari/537.36

1 / 190 requests | 455 B / 4.2 MB transferred | 42
```

(a) “stateless” crawl of Kaiser Permanente

[30] I used Chrome version 116 Guest mode for both crawls.



Filter: google.com

```
Name
www.google.com
gen_204?s=webhp&t=aft&atyp=csi&ei=F8fiZP...
client_204?atyp=i&biw=821&bih=1245&ei=F8fi...
callout?prid=19037050&pgid=19037049&puid=...
cb=gapi.loaded_0
gen_204?atyp=i&ei=F8fiZPGAO7ze0PEPjP2tg...
client_204?cs=1&opi=89978449
gen_204?atyp=csi&ei=F8fiZPGAO7ze0PEPjP2t...
gen_204?atyp=csi&ei=GMfiZKuPEo650PEP8L...
gen_204?atyp=csi&ei=F8fiZPGAO7ze0PEPjP2t...
log?format=json&hasfast=true&authuser=0
gen_204?atyp=csi&ei=F8fiZPGAO7ze0PEPjP2t...
ui
gen_204?atyp=i&ct=psnt&cad=&nt=navigate&e...
favicon.ico
gen_204?use_corp=on&atyp=i&zx=169258370...
log?format=json&hasfast=true&authuser=0
log?format=json&hasfast=true
gen_204?atyp=i&ei=F8fiZPGAO7ze0PEPjP2tg...
gen_204?atyp=i&ei=F8fiZPGAO7ze0PEPjP2tg...
gen_204?atyp=i&ei=F8fiZPGAO7ze0PEPjP2tg...
?random=1692583721367&cv=11&fst=169258...

22 / 227 requests | 111 kB / 5.3 MB transferred
```

```
Content-Length:              42
Content-Security-Policy:     script-src 'none'; object-src 'none'
Content-Type:                image/gif
Cross-Origin-Resource-       cross-origin
Policy:
Date:                        Mon, 21 Aug 2023 02:08:41 GMT
Expires:                     Fri, 01 Jan 1990 00:00:00 GMT
P3p:                         policyref="https://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA
                             PSD IVA IVD OTP OUR OTR IND OTC"
Pragma:                      no-cache
Server:                      cafe
Timing-Allow-Origin:         *
X-Content-Type-Options:      nosniff
X-Xss-Protection:            0
▼ Request Headers
:authority:                  www.google.com
:method:                     GET
:path:                       /pagead/1p-user-list/881418786/?
                             random=1692583721367&cv=11&fst=1692583200000&bg=ffffff&guid=ON&async=1&gt
                             m=45be38g0&u_w=3440&u_h=1440&url=https%3A%2F%2Fhealthy.kaiserpermanente.
                             org%2Fnorthern-california%2Ffront-
                             door&frm=0&tiba=Custom%20Care%20%26%20Coverage%20Just%20For%20You%2
                             0%7C%20Kaiser%20Permanente&data=event%3Dgtag.config&fmt=3&is_vtc=1&rando
                             m=266773835&rmt_tld=0&ipr=y
:scheme:                     https
Accept:                      image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:             gzip, deflate, br
Accept-Language:             en-US,en;q=0.9
Cookie:                      1P_JAR=2023-08-21-02;
                             NID=511=BNimS1Gw5OkuM6RDPZOewGnoicsUWBMwhjN1iaPptvVBZW9nLjsUPHibAJ
                             vN48Y0Zq75926m_j_z6UozBpCIO28QQeRPnBy_SsZR3qjKqqQtj5HmOpYwkoTi5cVbz2
                             TYt8WTw8oX175vYzLlq8e588hQGbvdQqKRJRAF0z-rtkq5i7HciCf6EQ
Referer:                     https://healthy.kaiserpermanente.org/
Sec-Ch-Ua:                   "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Sec-Ch-Ua-Mobile:            ?0
Sec-Ch-Ua-Platform:          "macOS"
Sec-Fetch-Dest:              image
Sec-Fetch-Mode:              no-cors
Sec-Fetch-Site:              cross-site
User-Agent:                  Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
                             Gecko) Chrome/116.0.0.0 Safari/537.36
```

(b) "stateful" crawl of Kaiser Permanente website after visiting www.google.com

Figure 8: Cookie transmissions to Google in "stateless" vs. "stateful" crawls

41. Thus, the absence of third-party cookies in Dr. Zervas' testing results can be attributed to his flawed ("stateless") methodology, rather than an accurate reflection of real-world network data transmissions.

42. Dr. Zervas also misrepresents Google's disguised use of "first-party" cookies. He states that "Plaintiffs allege that Google disguises cookies used in relation to provision of its services as first-party cookies when in reality they are third-party cookies. That allegation conveys a fundamental misunderstanding of how cookies operate and are used by Google and developers." He goes on to say that "Google's reliance on first-party cookies set and transmitted by web properties is not Google's attempt to circumvent user privacy, as alleged." (Zervas Declaration ¶30).

43. Dr. Zervas seems to be unaware of the phenomena of cookie ghostwriting. While he admits that "the website can still send the cookie value to a third party, such as Google Analytics"

(Zervas Declaration ¶ 31), he fails to recognize that it is not "the website" but rather the Google Analytics source code that sends "first-party" cookies to Google Analytics.

44. Over the past several years, numerous peer-reviewed research studies have shown how trackers ghostwrite "first-party" cookies. The concept of cookie ghostwriting pertains to cookies that are set on behalf of a first-party (i.e., the website the user is currently visiting) but are actually written by a different entity (e.g., a third-party script).

45. Ghosted cookies present a covert means of tracking, as they can trace even those privacy-conscious users who block third-party cookies, through the use of "first-party" ghosted cookies.

46. Google Analytics' "first-party" cookies such as _ga and _gid are in reality ghostwritten by third-party Google Analytics' JavaScript source code.

47. Peer-reviewed research[31] studying "first-party" ghostwritten cookies shows that Google's JavaScript source code ghostwrites "first-party" cookies on 93% of the 415,545 websites where it is present. Google was identified as the leading ghostwriter of "first-party" cookies on the web.

48. Peer-reviewed research[32] that studied the abuse of "first-party" cookies for tracking, when third-party cookies are blocked, has reached similar conclusions. The study showed that Google is responsible for ghostwriting "first-party" tracking cookies on 77% of the top websites. These are then exfiltrated to hundreds of both Google-owned and non-Google domains. Note that two most widely used ghostwritten "first-party" cookies on the web include the two Google Analytics cookies: (1) _gid cookie set by Google Analytics on 77% of the websites and exfiltrated to 56 third-party domains; (2) _ga cookie set by Google Analytics on 69% of the websites and exfiltrated to 179 third-party domains. This shows

[31] Sanchez-Rola, I., Dell'Amico, M., Balzarotti, D., Vervier, P. A., & Bilge, L. (2021, May). Journey to the Center of the Cookie Ecosystem: Unraveling Actors' Roles and Relationships. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1990-2004). IEEE.

[32] Munir, S., Siby, S., Iqbal, U., Englehardt, S., Shafiq, Z., & Troncoso, C. (2023, January). CookieGraph: Understanding and Detecting First-Party Tracking Cookies. In ACM Conference on Computer and Communications Security (CCS).

that Google's ghostwritten "first-party" cookies are not only being used by Google to track users but also to help hundreds of other third parties for tracking.

49. Mr. Ganem asserts that "Google Analytics does not associate IP address […] with any specific individual" (¶37). First, he is tacitly admitting that Google Analytics – until recently[33] – used to collect IP addresses by default. Specifically, he states that "The prior version of Google Analytics for websites, Universal Analytics, allows a developer to request masking of the IP addresses it is collecting" (¶37).

50. Note that IP masking was not the default option, and that IP masking only removes the last few bits of the IP address.[34] Even with IP masking, Google Analytics still collected 24 bits and 48 bits for IPv4 and IPv6, respectively.

51. Mr. Ganem also leaves out a crucial fact that Google's other third-party products (e.g., Google Ads, Google Display Ads, Google Ad Manager) still continue to collect IP address in various transmissions (e.g., transmissions to adservice.google.com and doubleclick.net).

52. Dr. Zervas states that "Dr. Shafiq ignores how IP addresses are actually allocated, used (or reused), or shared among users. The logic Dr. Shafiq presents is incorrect." (Zervas Declaration ¶ 193).

53. Dr. Zervas fails to provide any evidence or original analysis, instead relying on hypothetical toy examples. In contrast, to support my conclusions, I cite various peer-reviewed scientific research studies that leverage large-scale empirical measurements. I expand on my explanations and provide additional scientific evidence to support my original conclusion and refute Dr. Zervas' conclusion below:

    a. Regarding IPv4, peer-reviewed scientific research shows that IP address can be used to identify users over time: "87% of participants retain at least one IP

[33] [GA4] Introducing the next generation of Analytics, Google Analytics 4 https://support.google.com/analytics/answer/10089681?hl=en

[34] IP masking in Universal Analytics https://support.google.com/analytics/answer/2763052

address for more than a month". For the study participants in the United States, the average IP address retention period was 18.93 days.[35]

b. Regarding IPv6, peer-reviewed scientific research shows that parts of IPv6 addresses (i.e., prefixes) of residential Internet subscribers can remain stable for months, permitting long-term use of 64-bit IPv6 prefixes to identify users at the household level (i.e., the router inside a home). In fact, the researchers found that these household-IPv6 prefixes are even more stable than IPv4 addresses.

c. Dr. Zervas further attempts to cite an observation from a peer-reviewed study that I cited in my initial report, but presents a mistaken conclusion because he confuses uniqueness with persistence. He states that "At the same time, one individual may be associated with multiple IP addresses (e.g., work and home). Indeed, the peer-reviewed research Dr. Shafiq cites relies on the data of '34,488 unique public IP addresses collected from 2,230 unique users'—which is more than 15 IP addresses per studied user on average, further discrediting Dr. Shafiq conclusions." (Zervas Declaration ¶ 140). He fails to recognize that multiple IP addresses per studied user does not imply that IP addresses are not unique or near-unique. Put simply, even if the IP addresses change, as long as they are sufficiently unique and persistent during a time period, they can be used for tracking as the authors of the paper concluded. To be clear, here is the final conclusion of the authors of the paper that Dr. Zervas relies on: "Our analysis shows that 93% of users in our dataset had a unique set of long-lived IP addresses (minimum retention period of 30 days) that remain stable over time"[36] The authors conclusion contradicts Dr. Zervas' assertions.

[35] Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R., & Lopatka, M. (2020, April). Don't count me out: On the relevance of IP address in the tracking ecosystem. In Proceedings of The Web Conference 2020 (pp. 808-815).

[36] *Id.*

d. Dr. Zervas applies the same erroneous conclusion to other identifiers Google stores in cookies by stating "this conclusion is also broadly applicable to many types of data besides an IP address that Dr. Shafiq considers. For example, cookie values can be reset or expire (see Section IV.C.3)." (Zervas Declaration ¶ 140). First, even if a user identifier stored in cookie values is reset or expires, it remains a unique identifier for that user. Second, for an identifier to be useful, it has to be persistent for a reasonable time, not permanent. The cookies used by Google do not expire for several hours, days, weeks, or even years. For example, the lifetimes of the _ga, _gid, IDE, DSID, and NID cookies are 2 years, 24 hours, 13 months, 2 weeks, and 6 months, respectively.

54. To rebut my conclusion that "Google can combine different data to identify individual users" (Zervas Declaration ¶137), Dr. Zervas points out that "Dr. Shafiq assumes that the attributes contained in the transmissions from healthcare web properties to Google (such as IP address, screen size and color depth, screen resolution) are independent." (Zervas Declaration ¶142). This is again a false assertion.

55. I explicitly recommend using joint entropy that considers the dependence between different data elements (Shafiq Declaration ¶ 13). In trying to support his false assertion, Dr. Zervas misinterprets a peer-reviewed paper[37] that I cited to show that various attributes can be combined to uniquely identify users. Specifically, Dr. Zervas first attempts to add entropy of various types of data to over 50 bits and then suggest that "the paper concludes that such data contain only around 18.8 bits of information after accounting for the fact that those types of data have much less unique information not already present in other types of data" (Zervas Declaration ¶143). Dr. Zervas then concludes these 18.8 joint entropy bits do not surpass the "32 bit identifiability threshold", and hence the information is not identifiable.

[37] Eckersley, P. (2010). How unique is your web browser?. In Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10 (pp. 1-18). Springer Berlin Heidelberg.

56. Dr. Zervas fails to recognize a basic fact that the threshold is based on the size of the population. The 32 bit identifiability threshold is based on the 4.6 billion web users assumption by Google employees in their analysis.[38] Given that the number of browsers considered in the study was N = 470,161, the joint entropy needed to uniquely identify a user in a population of size N is $\log_2(N)$ = 18.8 bits. In other words, the joint entropy computed by the authors meets the identifiability threshold for the considered population in their study.

V. OPINION # 3: GOOGLE CAN AND DOES IDENTIFY HEALTHCARE PROVIDER PROPERTIES AND SENSITIVE HEALTH INFORMATION

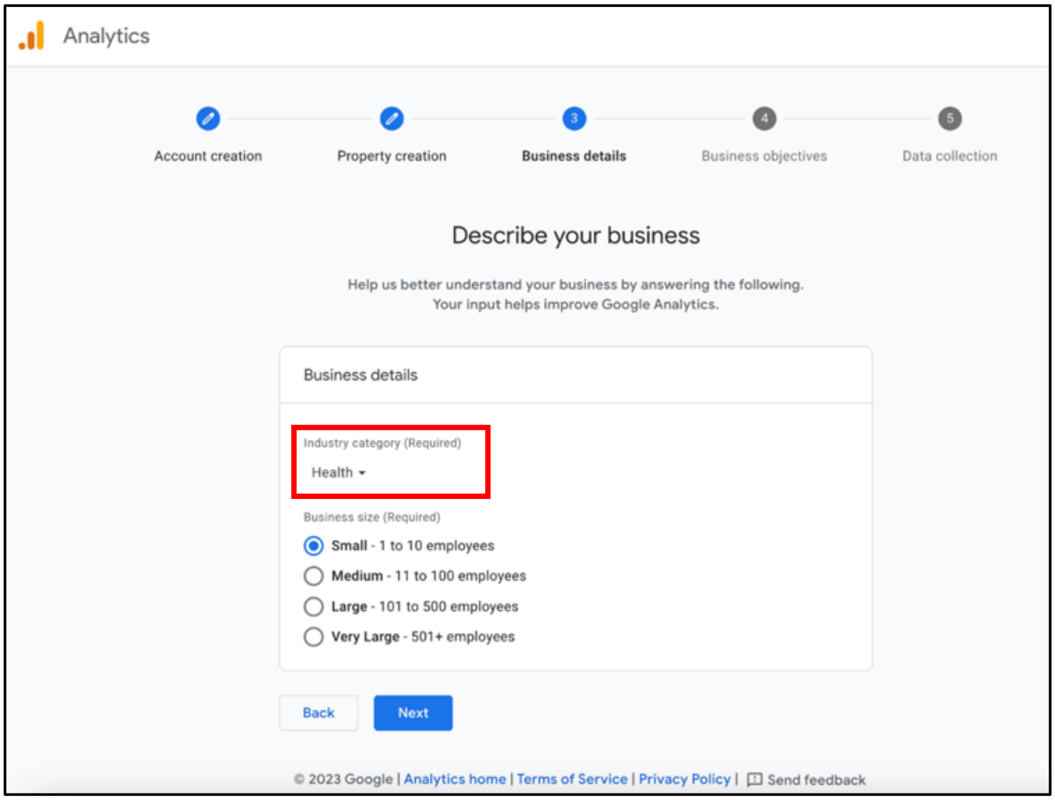
57. The Zervas, Ganem, and Takabvirwa Declarations misrepresent Google's ability and practices to identify healthcare provider properties and detect sensitive health information.

58. Mr. Ganem states that "There are millions of websites and apps that use Google Analytics. Google Analytics is not aware which, if any, of its developers are "healthcare providers," and does not have a list of "healthcare provider" websites and apps." (Ganem Declaration ¶ 51). Dr. Zervas states that "websites classified as "sensitive" by Google's internal classification tools, such as healthcare provider websites, cannot use Google's personalized advertising services" (Ganem Declaration ¶ 16). These statements of Mr. Ganem and Dr. Zervas seem to contradict each other.

//
//
//

[38] FAQ Privacy Budget: https://github.com/mikewest/privacy-budget/blob/4e5f78adde92bd622dafeceae78682fc0823c0eb/faq.md

59. Mr. Ganem is wrong here. Google (and specifically Google Analytics) can and does identify healthcare provider properties. As shown in Figure 9, Google explicitly asks developers about their business details when they sign-up for Google Analytics. In a required field named "industry category", one of the choices Google offers is "Health". Given that healthcare websites would select this option, Google has a list of "Health" websites that use Google Analytics.



Describe your business

Help us better understand your business by answering the following.
Your input helps improve Google Analytics.

Business details

Industry category (Required)
Health ▾

Business size (Required)

● **Small** - 1 to 10 employees
○ **Medium** - 11 to 100 employees
○ **Large** - 101 to 500 employees
○ **Very Large** - 501+ employees

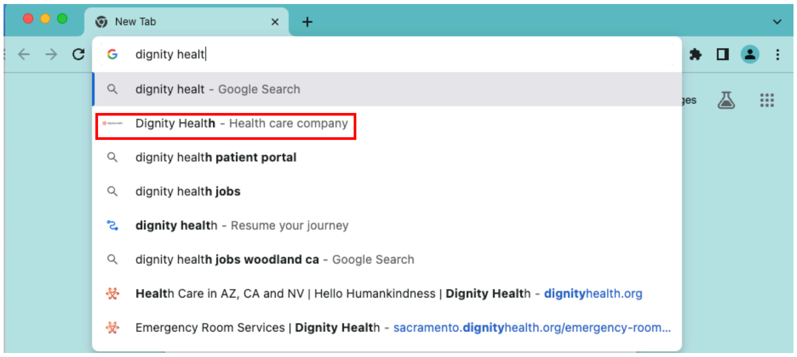
Figure 9: Google Analytics requires developers to disclose their business details including whether the industry category is "Health".

60. Google's mission is to "organize the world's information".[39] Its main products such as Search and Advertising would simply not work if Google was unable to categorize each property (website or app) and its contents. So, any assertion that Google is not aware of healthcare related properties is false. To drive the point home, I describe several publicly

[39] Google Search: Our approach to Search https://www.google.com/search/howsearchworks/our-approach/

available Google products that do this on a routine basis. There are likely several more internal (i.e., not public facing) Google systems that can do this as well.

a. Google's Chrome browser shows to its users whether they are about to visit a "Health care company". Specifically, the autocomplete feature in Google Chrome is able to do so even before a user types in the full website address. A couple of examples are shown in Figure 10:



dignity healt

dignity healt - Google Search

Dignity Health - Health care company

dignity health patient portal

dignity health jobs

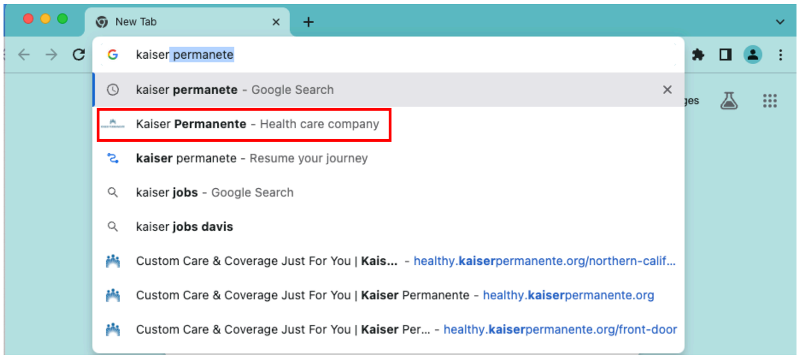
dignity health - Resume your journey

dignity health jobs woodland ca - Google Search

Health Care in AZ, CA and NV | Hello Humankindness | Dignity Health - dignityhealth.org

Emergency Room Services | Dignity Health - sacramento.dignityhealth.org/emergency-room...

Dignity Health – "Health care company"



kaiser permanete

kaiser permanete - Google Search

Kaiser Permanente - Health care company

kaiser permanete - Resume your journey

kaiser jobs - Google Search

kaiser jobs davis

Custom Care & Coverage Just For You | Kais... - healthy.kaiserpermanente.org/northern-calif...

Custom Care & Coverage Just For You | Kaiser Permanente - healthy.kaiserpermanente.org

Custom Care & Coverage Just For You | Kaiser Per... - healthy.kaiserpermanente.org/front-door

Kaiser Permanente – "Health care company"

Figure 10: Google's Chrome browser classifies healthcare provider properties as "Health care company"

b. Google's advertising products employ "Verticals" for classifying website content, such as "/Health/Medical Facilities & Services/Hospitals & Treatment Centers".[40]

c. Google's public API, as detailed on their official documentation at https://cloud.google.com/natural-language/docs/categories, also enumerates

[40] Verticals https://developers.google.com/adwords/api/docs/appendix/verticals

categories like Doctors' Offices, Hospitals & Treatment Centers, Medical Procedures, and Physical Therapy, among others under the umbrella of "Medical Facilities & Services".

61. All of this evidence underlines the fact that Google already has the requisite expertise and technology to discern the nature of the content within the vast expanse of the internet, and specifically in this case, to accurately identify healthcare-related websites.

62. Dr. Zervas states that "Google lacks sufficient information to determine whether certain content is sensitive […] developers are better informed about what information their web properties contain" (Zervas Declaration ¶ 66). Dr. Zervas contends that "[Google] lacks the necessary context to classify each data point within every webpage or application" (Zervas Declaration ¶ 135), further declaring that "While I concur that Google employs classification systems to categorize websites and applications for advertising objectives […] I deem Dr. Shafiq's desired application of one of these classification systems to pinpoint healthcare content to be ill-advised." (Zervas Declaration ¶ 145).

   a. First, Dr. Zervas fails to substantiate his statements with tangible evidence or reasoned explanation, leaving his claims unsupported.

   b. Second, Dr. Zervas appears to misrepresent the capabilities and practices of Google's classification systems. His assertion that "Google must classify each individual data point within each webpage or application" is misguided. In reality, Google's requirement extends merely to the classification of the specific webpage URL, a process that is more straightforward and efficient.

   c. The very first network request to Google that contains the healthcare website's URL provides the entire context that Google needs to classify it as healthcare-related or otherwise. Utilizing the classification systems that Dr. Zervas himself concedes Google possesses, this task is entirely feasible. Moreover, Google's classification systems can instruct the source code to cease all subsequent data collection, should it be deemed necessary. This can be executed through various mechanisms, such as by setting a "sensitive" flag in a browser cookie, akin to the method employed by DoubleClick in user opt-out scenarios.[41]

d. In his analysis, Dr. Zervas opines that "Google already uses multiple classification systems to prevent the use of sensitive information, including health-related information, in personalized ads." (Zervas Declaration ¶ 135). He further states that "Google's policies prohibit use of data from web properties classified as "sensitive" for personalized advertising or remarketing." (Zervas Declaration ¶ 146). Dr. Zervas' statements are tacit admissions that Google does indeed collect sensitive information, encompassing health-related data, and knows exactly when it does so. When Google's classification systems identify such sensitive information, the company becomes aware of its collection. Though Dr. Zervas states that this collected sensitive information is not utilized for personalized advertising or remarketing, the mere admission that Google can classify whether the information it collected is "sensitive", including that from healthcare providers, contradicts his earlier claim that "Google lacks sufficient information to determine whether certain content is sensitive" (Zervas Declaration ¶ 66).

VI. OPINION # 4: GOOGLE USES INFORMATION IT COLLECTS FROM HEALTHCARE PROVIDERS FOR PERSONALIZED ADVERTISING

63. The Zervas, Ganem, and Takabvirwa Declarations misrepresent Google's practices of using information it collects from healthcare provider properties for personalized advertising.

a. Mr. Takabvirwa suggests that "Google policy prohibits web domains and apps that are classified "Sensitive" from using advertiser-curated audience lists" (Takabvirwa Declaration ¶ 10) but at the same time explains that "Web domains and apps that are classified as "Sensitive" may use predefined Google audiences,

[41] Our advertising and measurement cookies https://business.safety.google/adscookies/

such as Affinity, Demographics, Detailed Demographics, Life Events, Location Targeting, and In-Market" (Takabvirwa Declaration ¶ 15).

b. Mr. Ganem asserts that "Google prohibits the use of medical information from personalized advertising" (Ganem Declaration ¶ 17).

c. Dr. Zervas recites Google policies explained in the Ganem and Takabvirwa Declarations, and attempts to conduct an experiment to show that Google personalizes ads on health-related websites only based on the contextual information (not behavioral information).

64. I respond to each of the above in turn.

65. Mr. Takabvirwa states that "web domains and apps that are classified as "Sensitive" may use predefined Google audiences, such as Affinity, Demographics, Detailed Demographics, Life Events, Location Targeting, and In-Market." (Takabvirwa Declaration ¶ 15). In other words, Mr. Takabvirwa admits that Google allows personalized advertising for sensitive websites, including healthcare provider websites. Consider "location targeting" at or near healthcare provider's physical location. Consider examples of a "life event" such as pregnancy or newborn that are related to healthcare and can be highly sensitive.[42]

66. Contrary to Mr. Ganem's above-mentioned assertion, there exists tangible evidence that Google does, in fact, serve personalized advertising based on health-related information. This fact is corroborated both by the contextually personalized ads acknowledged by Dr. Zervas in his testing (Zervas Declaration ¶50) and through my own independent analysis (discussed further below) that shows that Google does serve behaviorally targeted health-related ads, thus raising serious questions about the efficacy of Google's systems and policies designed to prevent the use of sensitive information, including health-related information, in personalized advertising.

[42] How Companies Learn Your Secrets https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

67. Dr. Zervas asserts that "Plaintiffs incorrectly frame contextual advertising as personalized advertising targeted using health information" (Zervas Declaration ¶ 50). Dr. Zervas seems to misunderstand the basics of ad personalization.

68. For starters, there are two main types of ad personalization: contextual and behavioral. In contextual personalization, ads are personalized based on the current context of the user such as content of the web page the user is on or the user's current location. In behavioral personalization, ads are personalized based on the user's past behavior such as browsing history or locations the user had visited in the past. Put simply, this means that contextual advertising is a form of personalized advertising. With respect to Dr. Zervas' Mayo Clinic example, since the Mayo Clinic's website was health-related, the ad on Mayo Clinic's website was contextually personalized based on health information on Mayo Clinic's website.

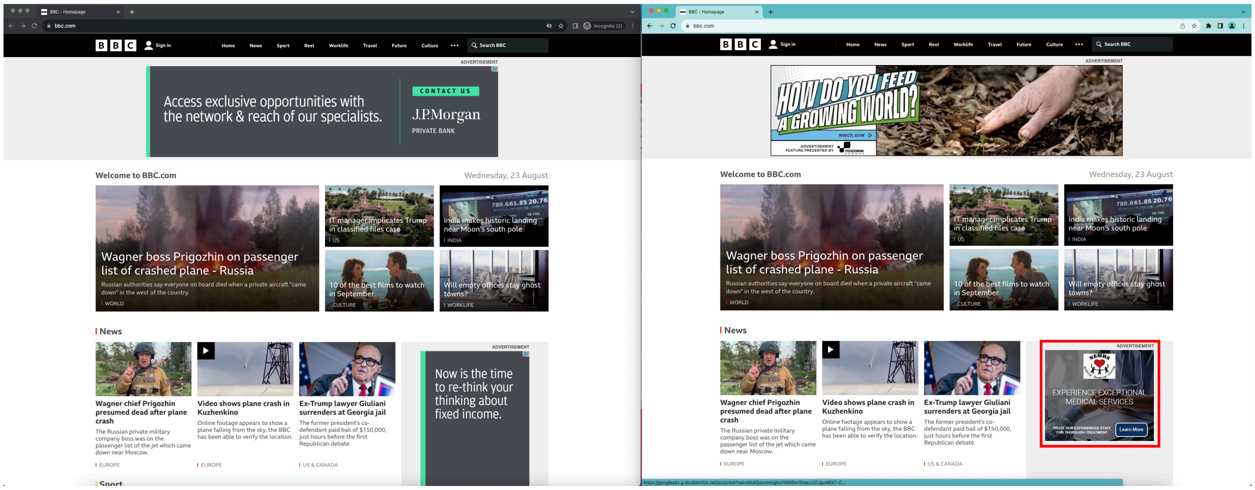
69. Dr. Zervas then goes on to conduct an experiment. He first visited Mayo Clinic's website after visiting Adidas' website in regular browsing mode. Then in a separate Incognito mode browser, he directly visited Mayo Clinic's website. When the same ad about Metastatic Breast Cancer showed up on Mayo Clinic's website in both browsers, Dr. Zervas concluded that this was a contextual ad and that "contextual ads can be displayed on websites, just as a billboard on the side of the road, and do not need to be personalized to a specific user" (Zervas Declaration ¶ 50).

70. I followed Dr. Zervas' methodology to illustrate that Google indeed does behaviorally target users with health-related ads. I first visited BBC's website after visiting the list of 3,394 healthcare provider websites in the regular Chrome browser.[43] Then in a separate Incognito mode Chrome browser, I directly visited BBC's website. The appearance of

[43] I created a fresh Chrome version 116 browser profile and then conduct a stateful crawl of the 3,394 Health Care Provider websites for "training". For "testing", I simply visited BBC.com (a generic website).

healthcare provider ads on BBC[44] cannot be explained as contextual using Dr. Zervas' logic.

71. Figure 11 shows side-by-side screenshots of the BBC's website across the pair of crawls. The left side is BBC's website in the Incognito browsing mode. The right side is BBC's website in the regular Chrome browser after visiting healthcare provider websites. The bottom ad on the right side (highlighted in the red box) is clearly behaviorally targeted because it belongs to Northeast Montana Health Services (https://nemhs.net), a site that was visited before visiting BBC's website. This is a textbook example of a remarketing ad based on the user's previous visit to a sensitive healthcare provider website.



Access exclusive opportunities with the network & reach of our specialists.

Welcome to BBC.com

Wednesday, 23 August

Wagner boss Prigozhin on passenger list of crashed plane - Russia

Russian authorities say everyone on board died when a private aircraft "came down" in the west of the country.

IT manager implicates Trump in classified files case

India makes historic landing near Moon's south pole

10 of the best films to watch in September

Will empty offices stay ghost towns?

News

Wagner chief Prigozhin presumed dead after plane crash

The Russian private military company boss was on the passenger list of the jet which came down near Moscow.

Video shows plane crash in Kuzhenkino

Online footage appears to show a plane falling from the sky, the BBC has been able to verify the location.

Ex-Trump lawyer Giuliani surrenders at Georgia jail

The former president's co-defendant paid bail of $150,000, just hours before the first Republican debate.

Now is the time to re-think your thinking about fixed income.

EXPERIENCE EXCEPTIONAL MEDICAL SERVICES

TRUST OUR EXPERIENCED STAFF FOR THOROUGH TREATMENT

https://googleads.g.doubleclick.net/pcs/click?xai=AKAOjsurmmghuYl6MSw15nauJJZJguABXT-C...

(left) directly visited BBC.com in the Chrome Incognito browsing mode

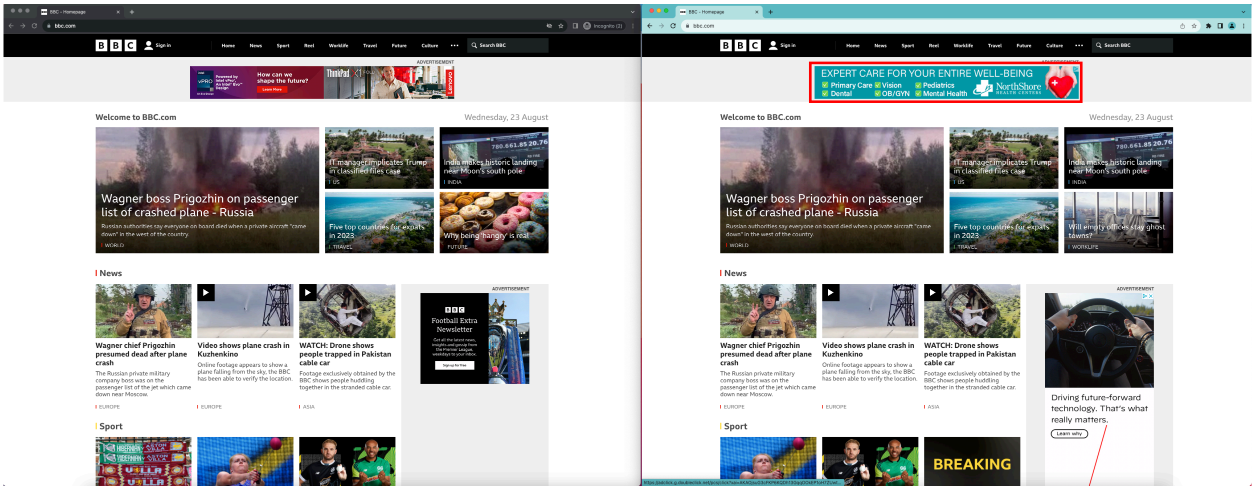
(right) visited BBC.com after visiting hospital websites in the regular Chrome browsing mode

Figure 11: Side-by-side screenshots of ads loading on BBC.com. Note the healthcare provider's (Northeast Montana Health Services) ad on the right side. Northeast Montana Health Services (https://nemhs.net) is in the list of the healthcare provider websites that were visited before BBC. This is evidence of behavioral remarketing based on the user's previous visit to a sensitive healthcare provider website.

72. Figure 12 shows side-by-side screenshots of the BBC's website across the pair of crawls. The left side is BBC's website in the Incognito browsing mode. The right side is BBC's website in the regular Chrome browser after visiting healthcare provider websites. The top

[44] Note that Google serves ads on BBC.com, as indicated by the URLs in the bottom left corner.

banner ad on the right side (highlighted in the red box) is clearly behaviorally targeted because it belongs to NorthShore Health (https://www.northshorehealthgm.org), a site that was visited before visiting BBC's website. This is another textbook example of a remarketing ad based on the user's previous visit to a sensitive healthcare provider website.


BBC
Welcome to BBC.com
Wednesday, 23 August
EXPERT CARE FOR YOUR ENTIRE WELL-BEING
✓ Primary Care ✓ Vision ✓ Pediatrics
✓ Dental ✓ OB/GYN ✓ Mental Health
NorthShore HEALTH CENTERS
Wagner boss Prigozhin on passenger list of crashed plane - Russia
IT manager implicates Trump in classified files case
India makes historic landing near Moon's south pole
Five top countries for expats in 2023
Why being 'hangry' is real
Will empty offices stay ghost towns?
News
Wagner chief Prigozhin presumed dead after plane crash
Video shows plane crash in Kuzhenkino
WATCH: Drone shows people trapped in Pakistan cable car
Football Extra Newsletter
Driving future-forward technology. That's what really matters.
Sport
BREAKING

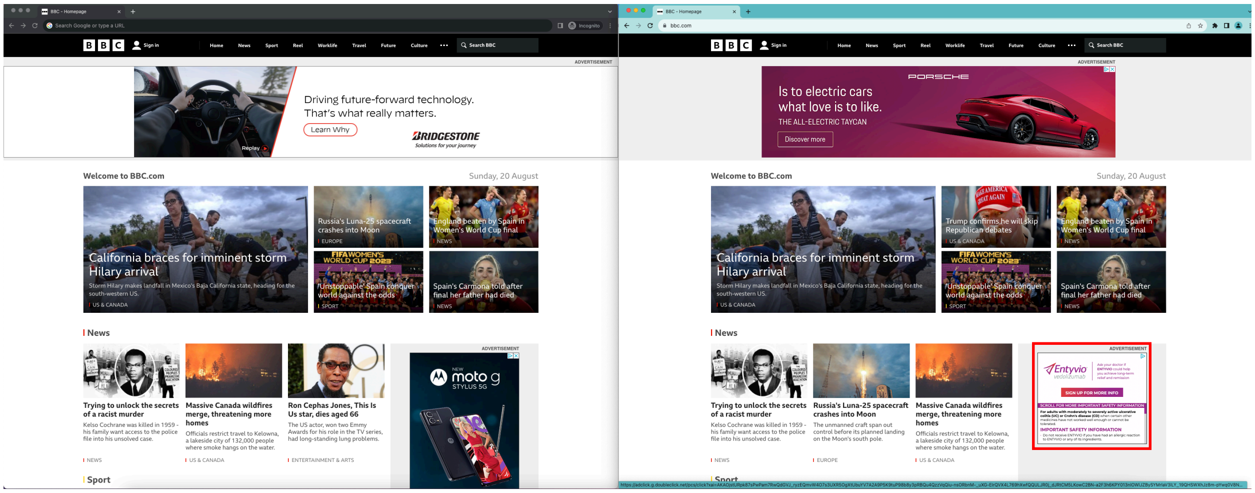
(left) directly visited BBC.com in the Chrome Incognito browsing mode

(right) visited BBC.com after visiting hospital websites in the regular Chrome browsing mode

Figure 12: Side-by-side screenshots of ads loading on BBC.com. Note the healthcare provider's (NorthShore Health) ad on the right side. NorthShore Health (https://www.northshorehealthgm.org) is in the list of the healthcare provider websites that were visited before BBC. This is evidence of behavioral remarketing based on the user's previous visit to a sensitive healthcare provider website.

//
//
//

73. Figure 13 shows side-by-side screenshots of the BBC's website across the pair of crawls. The left side is BBC's website in the Incognito browsing mode. The right side is BBC's website in the regular Chrome browser after visiting healthcare provider websites. The banner ad on the right side (highlighted in the red box) is a prescription medicine ad. This is example of a behaviorally targeted ad based on the user's previous visit to sensitive healthcare provider websites.



Driving future-forward technology. That's what really matters.

Welcome to BBC.com

Sunday, 20 August

California braces for imminent storm Hilary arrival

Storm Hilary makes landfall in Mexico's Baja California state, heading for the south-western US.

Russia's Luna-25 spacecraft crashes into Moon

England beaten by Spain in Women's World Cup final

FIFA WOMEN'S WORLD CUP 2023

'Unstoppable' Spain conquer world against the odds

Spain's Carmona told after final her father had died

News

Trying to unlock the secrets of a racist murder

Kelso Cochrane was killed in 1959 - his family want access to the police file into his unsolved case.

Massive Canada wildfires merge, threatening more homes

Officials restrict travel to Kelowna, a lakeside city of 132,000 people where smoke hangs on the water.

Ron Cephas Jones, This Is Us star, dies aged 66

The US actor, won two Emmy Awards for his role in the TV series, had long-standing lung problems.

Is to electric cars what love is to like.

THE ALL-ELECTRIC TAYCAN

Trump confirms he will skip Republican debates

The unmanned craft span out control before its planned landing on the Moon's south pole.

Ask your doctor if ENTYVIO could help you achieve long-term relief and remission

SCROLL FOR MORE IMPORTANT SAFETY INFORMATION

For adults with moderately to severely active ulcerative colitis (UC) or Crohn's disease (CD) when certain other medicines have not worked well enough or cannot be tolerated.

IMPORTANT SAFETY INFORMATION

- Do not receive ENTYVIO if you have had an allergic reaction to ENTYVIO or any of its ingredients.

https://adclick.g.doubleclick.net/pcs/click?xai=AKAOjstURpk87sPwPam7RwQdGVJ_ryzEQmvW4O7s3UXR5OgXtUbuYV7A2A9P5K9tuP98b8y3pRBQu4QzzVqQiu-nsORbnM-_uXG-ElrQVX4L769hXwfQQULJR0j_dJRtCM5LKowC2BN-a2F3h6KPY013nlOWIJZByS YMrlaV3lLY_19QHSWXhJz8m-pYwq0V8N...

(left) directly visited BBC.com in the Chrome Incognito browsing mode

(right) visited BBC.com after visiting hospital websites in the regular Chrome browsing mode

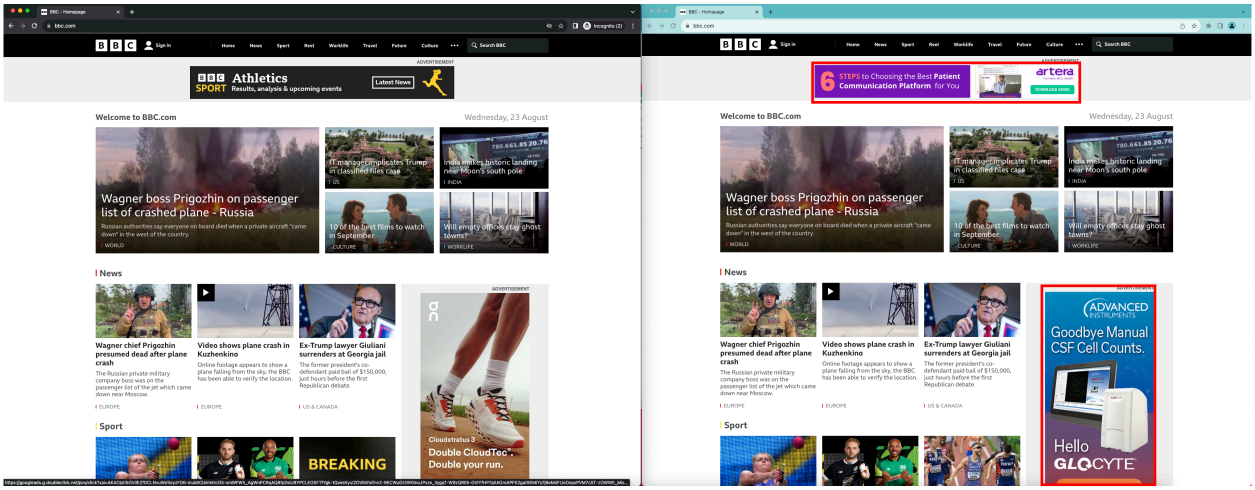
Figure 13: Side-by-side screenshots of BBC.com. Note the prescription medicine ad on the right side. This is evidence of behavioral targeting based on the user's previous visit to sensitive healthcare provider websites.

//

//

//

74. Figure 14 shows side-by-side screenshots of the BBC's website across the pair of crawls. The left side is BBC's website in the Incognito browsing mode. The right side is BBC's website in the regular Chrome browser after visiting healthcare provider websites. The ads on the right side (highlighted in the red box) are for medical equipment and services. This is an example of a behaviorally targeted ad based on the user's previous visit to sensitive healthcare provider websites.


BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
Future
Culture
Search BBC
ADVERTISEMENT
BBC SPORT Athletics
Results, analysis & upcoming events
Latest News
6 STEPS to Choosing the Best Patient Communication Platform for You
artera
Formerly WELL Health
DOWNLOAD GUIDE
Welcome to BBC.com
Wednesday, 23 August
Wagner boss Prigozhin on passenger list of crashed plane - Russia
IT manager implicates Trump in classified files case
India makes historic landing near Moon's south pole
10 of the best films to watch in September
Will empty offices stay ghost towns?
News
Wagner chief Prigozhin presumed dead after plane crash
Video shows plane crash in Kuzhenkino
Ex-Trump lawyer Giuliani surrenders at Georgia jail
Sport
BREAKING
Cloudstratus 3
Double CloudTec®.
Double your run.
ADVANCED INSTRUMENTS
Goodbye Manual CSF Cell Counts.
Hello GLOCYTE

(left) directly visited BBC.com in the Chrome Incognito browsing mode

(right) visited BBC.com after visiting hospital websites in the regular Chrome browsing mode

Figure 14: Side-by-side screenshots of BBC.com. Note the medical equipment and services ads on the right side. This is evidence of behavioral targeting based on the user's previous visit to sensitive healthcare provider websites.

//
//
//

75. In summary, there is evidence that Google uses information it collects from healthcare provider properties for personalized advertising, specifically behaviorally targeted advertising (e.g., remarketing). Google's policies to prohibit the use of information collected from sensitive (e.g., healthcare provider properties) for personalized advertising seem ineffective. Google's technical safeguards (if any) to prevent the use of information collected from sensitive (e.g., healthcare provider properties) for personalized advertising also seem inadequate.

* * *

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 24th day of August 2023 at Davis, California.

/s/ Zubair
Zubair Shafiq Ph.D.